Office of the
Privacy Commissioner
of Canada

Commissariat à la
protection de la vie privée
du Canada

Audit of the
Personal Information Management Practices of the
Canada Border Services Agency
Trans-border Data Flows

June 2006

TABLE OF CONTENTS

SECTION I

MAIN MESSAGES

1.1 We found that the Canada Border Services Agency (CBSA) has systems and procedures in place for managing and sharing personal information with other countries. However, significant opportunities exist to better manage privacy risks and achieve greater accountability, transparency and control over the trans-border flow of data. Trans-border data flows refer to personal information that is collected or disclosed across international borders.

1.2 Written requests for assistance from foreign governments are processed in accordance with requirements. However, many of the information exchanges between the CBSA and the United States at the regional level are verbal, and are not based on written requests. These exchanges are not recorded consistently and do not follow the approval process as established under CBSA policy. Furthermore, they are not compliant with the terms of the Canada-United States *Customs Mutual Assistance Agreement* of June 1984.

1.3 The CBSA needs a coordinated method of identifying and tracking all flows of its trans-border data. The Agency cannot, with a reasonable degree of certainty, report either on the extent to which it shares personal information with the United States, or how much and how often it shares this information. By extension, it cannot be certain that all information sharing activities are appropriately managed and comply with section 107 of the *Customs Act* and section 8 of the *Privacy Act*.

1.4 Generally, the controls surrounding the Passenger Information System (PAXIS) and the Integrated Customs Enforcement System (ICES) are sound. These two key systems contain sensitive personal information about millions of travellers. Notably, foreign jurisdictions do not have direct access to these systems, and electronic disclosures to the United States under the Shared Lookout and High-Risk Traveller Identification initiatives are transmitted over secure channels. However, there are opportunities to strengthen controls to further reduce the risk that personal information could be improperly used or disclosed. These opportunities include:

- completing the introduction of a new security management framework as initiated by the CBSA;
- updating and clarifying roles and responsibilities for IT functions;
- ensuring system access rights are kept up-to-date;
- implementing audit control capability for lookout data printouts; and
- introducing a mechanism for Canada and the United States to assure each other that the system controls and protection of shared personal information are adequate.

1.5 The CBSA needs to explore ways to improve the quality and control of data it acquires under the Advance Passenger Information/Personal Name Record (API/PNR) initiative to ensure that personal information is as accurate and complete as possible.

1.6 The CBSA has not yet evaluated the effectiveness of the High-Risk Traveller Identification (HRTI) Initiative with the United States because the project has yet to be fully implemented. In particular, it should assess the extent to which inaccurate or incomplete data may affect enforcement objectives and individual travellers. Until the CBSA has evaluated the initiative, the Agency will not be able to demonstrate that it has achieved its objective and, accordingly, that the collection and use of vast amounts of personal information about millions of travellers is justified.

1.7 The CBSA is a new entity. Therefore, the time is opportune for the Agency to articulate and implement a comprehensive privacy management framework. In particular, the CBSA should work toward updating and strengthening its agreements with the United States covering the sharing of personal information. The Agency should also consolidate its reporting of privacy incidents and look for ways of improving the monitoring of personal information disclosures.

1.8 Finally, the activities associated with sharing data across borders should be made more transparent. A clear and complete picture of these activities is not readily available to show what information is shared with whom, and for what purpose. As is true for other departments, the CBSA's trans-border data flows are not accounted for in meaningful detail. More transparency is needed to better inform Parliament and the Canadian public about activities in this area.

1.9 Addressing such matters is in the public interest. We believe that strong privacy management and accountability are essential for dealing with the public's concerns about the flow of personal information from Canada to other countries.

SECTION II

INTRODUCTION

Context for the Audit

2.1 The Canadian economy depends greatly on exchanging information with partners around the world. While Canada has many trading partners and allies, its strongest ties are with its closest neighbour – the United States of America.

2.2 Technological advances over the past two decades have removed many of the communication barriers for exchanging information. Data exchanges between multinational companies and national governments have increased with the expansion of database capacities and the creation of global communication systems and networks to transmit information.

2.3 Globalization has caused nations to adopt a more cooperative and coordinated approach to regulating goods and people and, in particular, information crossing their respective borders. This in turn has resulted in an increase in the sharing of personal information between national governments – something that was given added momentum in relation to law enforcement and national security following the tragic events of September 11, 2001.

2.4 In responding to the terrorist attacks of September 11, 2001, governments around the world – including the Government of Canada – introduced measures to strengthen national and international security. Generally, such measures seemed to be based on the premise that the more information governments have about individuals, the safer and more secure society will be.

2.5 Since the events of 9/11, calls have arisen for better sharing of information between law enforcement partners domestically and internationally to respond to the threat of terrorism. All law enforcement and intelligence agencies must balance heightened surveillance and security measures with competing calls for selective sharing and greater oversight to ensure that civil liberties – including the right of privacy – are not unnecessarily compromised. Nevertheless, travellers would generally understand that the degree of personal privacy at a port of entry into Canada will not be the same as may otherwise be the case in every day life. Scrutiny of people and goods by CBSA officials is to be expected, and it is provided for by law as a means of protecting the general welfare of Canada. Accordingly, screening and information sharing by the CBSA for purpose of border management takes place in a general context of reduced privacy.

2.6 We chose the CBSA for audit after considering a number of factors. Key components of the Government of Canada's national security agenda focus on strengthening the Canada-U.S. border, and the CBSA is the central organization responsible for border security in Canada. In December 2001, Canada and the United States signed the "Smart Border" Declaration – the *Manley-Ridge Smart Border Declaration and 30-Point Action Plan* to strengthen the shared border without unduly restricting legitimate trade and travel. A main objective of the plan was to explore options for increasing bilateral cooperation and the exchange of enforcement and intelligence information between the two jurisdictions.

2.7 In fulfilling its border protection mandate, the CBSA collects sensitive personal information about millions of travellers arriving in Canada. This information may include detailed financial, family history and travel information, as well as personal identifiers such as social insurance and passport numbers. Much of this information is retained in an identifiable format either in hard copy (physical files) or in electronic databases. This information may be exchanged with foreign governments under section 107(8) of the *Customs Act*.

2.8 The "Customs Action Plan" of April 7, 2000 articulated a new risk-based management approach to customs enforcement. The Plan focused on directing customs resources where they would produce the best results. This new enforcement method has led to the collection and use of large quantities of personal information about travellers, with the potential that the information may be shared across borders. When more personal information is collected, used and disclosed, corresponding privacy risks increase.

2.9 Finally, the Government of Canada's *National Security Policy* of April 27, 2004 included new funding for border security initiatives, including expanding the CBSA's intelligence gathering capacity and the creation of the National Risk Assessment Centre to facilitate the sharing of intelligence and lookout information with the United States (see paragraph 3.58 for a brief explanation of "lookouts").

Why this Audit is important

2.10 In an environment within which national governments are responsible for protecting the privacy rights of individuals, and in which many of these governments offer their citizens variable levels of protection, the trans-border flow of personal information raises unique privacy challenges. How, for example, can the Government of Canada, within the territorial limits of the application of its laws, ensure that information it shares with a foreign government will be accorded the same level of protection that the information enjoys in Canada? Will generally accepted data protection principles be recognized and respected?

2.11 More specifically, this audit is important for a number of reasons. First, the trans-border flow of personal information raises serious inherent privacy risks relating to jurisdictional differences in practices affecting the protection of personal information, the security of personal data in transit and the adequacy of instruments governing the management of the personal information once it has been shared. In this regard, we view the terms and conditions established under bilateral information sharing agreements to be important elements of the control environment surrounding trans-border data flows.

2.12 Second, there are clear indications that the Canadian public is concerned about the trans-border flow of their personal information to the United States. In a study commissioned by this office in 2004, 75% of respondents believed that the Government of Canada transfers citizens' personal information to foreign governments for the purpose of protecting national security, with 85% of those surveyed reporting a moderate or high level of concern about these transfers. In the same vein, many have raised trans-border concerns about data mining, racial profiling, direct access to Canadian databases by the foreign governments (notably the U.S.) and secondary uses of the information.

2.13 Third, as law enforcement and national security organizations around the world collect more information from more sources about more individuals, and as they use that information to identify possible threats, there is an inherent risk of incomplete or inaccurate data leading to undesirable consequences such as unnecessary scrutiny of individuals.

About the Canada Border Services Agency

2.14 The Canada Border Services Agency (CBSA) was created on December 12, 2003. It is part of the Public Safety and Emergency Preparedness (PSEP) portfolio. The CBSA encompasses the customs program from the former Canada Customs and Revenue Agency (CCRA), the enforcement, intelligence and interdiction functions of Citizenship and Immigration Canada (CIC) and the primary food and plant inspection functions of the Canadian Food Inspection Agency (CFIA).

2.15 The CBSA's legislative mandate is to facilitate the legitimate cross-border flow of people and goods in support of the Canadian economy, while intercepting those individuals and goods that pose a potential security risk to Canada or its allies, or who are not complying with Canadian customs, immigration and other laws. The CBSA administers more than 90 statutes governing trade and travel.

2.16 By serving as a first line of defence in managing the movement of people and goods entering and leaving Canada, the CBSA operates at some 1,200 service points across the country and 39 locations abroad. It is present at 119 land border crossings and nine international airports. Over the past fiscal year, the CBSA's staff of approximately 12,500 processed over 12 million shipments and 95 million travellers arriving in Canada – whether by land, air or water. In the same period, the Agency processed more than 2 million people referred for immigration reasons.

2.17 The CBSA's headquarters is in Ottawa. Its operations are divided into eight regions – Atlantic, Quebec, Greater Toronto Area, Niagara Falls/Fort Erie, Windsor/St. Clair, Northern Ontario, Prairie and Pacific.

2.18 The CBSA had a budget of $1.06 billion to carry out its border mandate for the fiscal year ending March 31, 2005. More information about the CBSA can be obtained from reports published on its website at www.cbsa-asfc.gc.ca.

2.19 When we were carrying out our audit, the CBSA was organizing as a new entity. Accordingly, systems and procedures required adjusting and were changing. We recognize that during a period of transformation there is much to be done, and officials were working hard to learn and adapt. At the same time, there can be some confusion or uncertainty among management and staff about roles and responsibilities and how corporate systems should and do operate. Nevertheless, it should also be understood that trans-border data flows are central to many of the Agency's programs and the day-to-day operations. Neither the Agency nor the federal government as a whole has, as yet, focused on these flows as a collective management and accountability issue.

Audit objective, criteria, scope and approach

2.20 National security and privacy objectives are often perceived as values to be balanced against each other – where, for example, increased security must result in a corresponding loss of privacy. The premise of this audit is that national security objectives and sound personal information management practices are mutually dependent.

2.21 Underlying this hypothesis is the belief that a strong accountability and control framework over the management of personal information will mitigate privacy risks, and it will also support national security and law enforcement objectives. In other words, security that respects privacy makes for better, more effective security.

Audit objective:

To assess the extent to which the CBSA is adequately controlling and protecting the flow of Canadians' personal information to foreign governments or their institutions.

Criteria:

2.22 Detailed criteria were developed for the audit. These were shared with the CBSA and accepted. The criteria are found in Appendix B (page 59). In establishing the audit criteria, reference was made to:

- the relevant authorities of the *Customs Act* (e.g., section 107);
- the collection, use, disclosure, retention and disposal provisions contained in sections 4 to 8 of the *Privacy Act*;
- the ten internationally recognized fair information principles embodied in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA); and
- Treasury Board policies, guidelines and directives relating to the management of personal information.

Scope:

2.23 Due to the size and complexity of the CBSA and its current state of reorganization, our audit began with a scoping review of the Agency's many programs and information management activities. We carried out this exercise to identify the program areas where the impact on individual privacy of Canadians would likely be highest so as to direct our attention accordingly. Mindful of our available audit resources, scoping activities were directed at the management of personal information about individual travellers rather than at the CBSA's commercial programs and activities. In addition, we focused on customs enforcement and intelligence activities at land borders and airports. The scope of the examination did not include the Agency's marine, rail and postal operations.

2.24 Our scoping activities led us to select the following four program areas and information systems for audit examination:

- Customs enforcement and intelligence activities (land borders and airports);
- the Integrated Customs Enforcement System (ICES);

- the Passenger Information System (PAXIS); and
- the National Risk Assessment Centre (NRAC).

2.25 In addition to these four areas, the audit examined the CBSA's privacy management framework, as well as the extent to which the Agency reports its activities in the area of trans-border data flows to Parliament and the Canadian public.

2.26 Although immigration enforcement, intelligence and interdiction activities also involve the trans-border flow of personal information, the organizational changes required to facilitate the integration of these activities into the CBSA had not been finalized at the time of our audit. This also applies to the primary food and plant inspection program that was transferred to the CBSA from the CFIA. These areas were, therefore, not examined as part of the audit.

2.27 Further, we did not review the NEXUS program. This program involves extensive background screening to facilitate accelerated entry into Canada and the United States for approved travellers. Enrolment in the NEXUS program is voluntary. Moreover, the collection, use and disclosure of personal information under the program occur with the expressed consent of the participant.

2.28 As a final note, the Privacy Commissioner does not have jurisdiction outside Canada. Therefore, we did not audit the control and use of personal information once it had crossed the Canada-U.S. border into the United States.

Approach:

2.29 We carried out interviews with 108 CBSA staff members. The interviewees included senior managers and program officers at CBSA Headquarters, managers and staff of the National Risk Assessment Centre, regional directors, divisional chiefs, customs superintendents, customs officers, regional intelligence officers, regional intelligence analysts and regional customs investigators in the three regions visited during the audit – Quebec, Windsor-St. Clair and Pacific.

2.30 In addition to interviewing selected personnel, the audit team examined a sample of customs enforcement records (e.g., seizure reports), intelligence management system (IMS) file entries, officer notebooks, requests for assistance files and Canada-U.S. shared lookouts. As the CBSA does not currently have the capacity to readily identify all files containing trans-border exchanges – specifically those that contain information that has been the subject of a verbal disclosure – the audit team was unable to randomly select certain types of files for review. Rather, we had to rely upon program officials to present records for our examination, the selection of which was based on officers' recollection of specific cases and manual searches of their respective records (e.g., notebooks).

2.31 The audit team also reviewed memoranda of understanding (MOUs) and treaties that establish the framework for disclosing (i.e., releasing) customs information to foreign governments, internal policies and procedures, training materials, privacy impact assessments and the CBSA's reporting instruments (e.g., Reports on Plans and Priorities).

2.32 Our field examination of the CBSA was substantially completed by November 2005. Therefore, the observations and recommendations contained in this report are effective as of that date.

2.33 As part of our approach, an external Audit Advisory Committee was established. This four-person committee brought extensive expertise in the areas of privacy, law enforcement, information technology security and public administration. The Committee provided guidance and direction at various stages of the audit.

2.34 After we had completed the examination phase of the audit, we provided verbal briefings of our findings to management of the CBSA. Drafts of our report were reviewed by CBSA officials to ensure factual accuracy and to obtain responses to our observations and recommendations.

2.35 Some of our audit observations relate to matters that are particularly sensitive in nature and have been excluded from this public report in the interest of maintaining information security of the CBSA. The observations and recommendations have been reported separately to the CBSA by management letter. We will be monitoring the Agency's efforts to address these matters as part of our follow-up to this audit report.

2.36 We wish to thank CBSA officials for their cooperation during the audit and their receptiveness to our work.

Organization of this report

2.37 Section III of this report, – Observations and Recommendations – follows and covers the four program areas and information systems noted earlier: customs enforcement and intelligence activities (land borders and airports); the Integrated Customs Enforcement System (ICES); the Passenger Information System (PAXIS); and the National Risk Assessment Centre (NRAC). For each, as appropriate, we provide some background or briefly describe the program, initiative or system. Then, observations relating to the trans-border flow of personal information and disclosure to foreign governments are discussed under separate sub-headings. Finally, we present the recommendations associated with a given set of observations.

Audit team

Trevor Shaw – Director General, Audit & Review

Tom Fitzpatrick
Michael Fagan
Robert Bedley
Douglas Marshall

External Audit Advisory Committee Members

John L'Abbe	Security Strategist Consultant, L'Abbe Consulting Services (Former Assistant Commissioner, RCMP – Retired)
John Hopkinson	IT Security Consultant EWA Information & Infrastructure Technologies, Inc.
David Flaherty	Privacy and Information Policy Consultant (Former Information and Privacy Commissioner of British Columbia)
Denis Morency	Independent Privacy Consultant (Former Director General, Information and Privacy Commissioner of Quebec)

SECTION III

OBSERVATIONS and RECOMMENDATIONS

CUSTOMS ENFORCEMENT AND INTELLIGENCE ACTIVITIES (LAND BORDERS AND AIRPORTS)

Background

3.1 The key components of the CBSA's enforcement presence are the investigations, intelligence and interdiction programs designed to address suspected cases of duty evasion, smuggling, fraud, terrorism, money laundering and other offences against laws that the Agency enforces.

3.2 The Enforcement Branch at CBSA Headquarters is responsible for developing national procedures, strategies and operational policies related to the Agency's enforcement program.

Other responsibilities include:

- collecting, analyzing and disseminating intelligence regarding threats to the security of Canada's borders;
- providing functional direction and support to CBSA field staff at ports of entry and inland offices;
- providing a focal point for the CBSA's relations with domestic and foreign security, law enforcement and intelligence communities; and
- developing and managing new programs with international partners.

3.3 The Branch is organized into four Directorates – Enforcement, Intelligence and Risk Management, Policy and Program Development, and Management Services. While CBSA Headquarters provides policy and functional direction to the field, the responsibility for delivering the enforcement program resides at the regional level. The CBSA's regional heads have management oversight of the border security and intelligence operations of their respective jurisdictions.

3.4 Enforcement operations include managing air, land and sea ports of entry for the movement of travellers and goods. Although the organizational structure may vary slightly from region to region, the enforcement programs all contain the same general components – that is, intelligence (customs and immigration), investigations (customs fraud) and immigration enforcement.

Personal information

3.5 The *Customs Act* defines "customs information" as information of any kind and in any forms that:

(a) relates to one or more persons and is obtained by or on behalf of the Minister for the purposes of the *Customs Act* or the *Customs Tariff;* or
(b) is prepared from information described in paragraph (a).

3.6 By definition, customs information is broad in scope. While not exhaustive, the following represents a sampling of the type of personal information that the CBSA collects and, by extension, could potentially be the subject of a trans-border disclosure:

- biographical information – name, date and place of birth;
- address and telephone numbers (home, cellular);
- previous customs violations;
- intelligence – methods of concealment, modus operandi of the individual, commodity data pertaining to goods likely to be smuggled, travel history and surveillance notes; and
- other information such as vehicle licence number, advance passenger information (API), passenger name record (PNR), employment and financial information.

Trans-border flow of personal information

3.7 In carrying out its border protection mandate, the CBSA collects personal information from a variety of sources. In addition to direct collection – that is from the person to whom the information relates – the CBSA collects information from air carriers, other government departments and agencies, domestic law enforcement and intelligence agencies, and foreign governments and their institutions. It also receives information from members of the general public through a toll-free tip line.

3.8 The CBSA may also collect information through leads that originate from customs ports of entry, surveillance activities, human sources and the execution of warrants. In addition, the CBSA has access to information contained in a number of external databases. These include the Canadian Police Information Centre (CPIC); Field Operational Support System (FOSS) – a Citizenship and Immigration Canada database; the Police Information Reporting System (PIRS), which is being replaced with the Police Reporting and Occurrence System (PROS); and the U.S. National Crime Information Centre (NCIC), the U.S. equivalent to the Canadian CPIC system.

3.9 Personal information collected under the CBSA's customs enforcement program is retained in hard copy (paper) and electronic formats. In addition to the PAXIS and ICES applications (examined as part of the audit), enforcement personnel may, depending on their role and area of responsibility, use the following systems in carrying out their duties:

Occurrence Reporting System (ORS)	–	an electronic reporting system for transmitting information from customs inspectors to intelligence personnel,
Intelligence Management System (IMS)	–	the repository for all intelligence data, with access being restricted to intelligence personnel,
Customs Investigations Information Management System (CIIMS)	–	a case management tracking system used by investigations staff, which captures case summary, tombstone data (name, address, DOB), date of port prosecution.

Disclosure to foreign governments

3.10 Subsection 107(8) of the *Customs Act* permits the disclosure of customs information to a foreign government, an international organization established by the government of states, a community of states, or an institution of any such government or organization. Any release of information must be:

- in accordance with an international convention or agreement, or other written arrangement between the Government of Canada or institution thereof and the foreign government, international organization or community of states; and
- solely for the purposes set out in the arrangement.

3.11 International information sharing agreements do not have to deal exclusively with the exchange of customs information. However, they must allow for the disclosure or exchange of such information.

3.12 Many bilateral agreements between customs agencies in different countries are designed to establish protocols governing their mutual assistance and cooperation. Canada has 20 international written collaborative arrangements. Six of these arrangements are Customs Mutual Assistance Agreements (CMAA). A CMAA must be ratified by Order-in-Council, has treaty status and is enforceable in law. Such agreements are government to government. Canada has a CMAA with the United States of America, Mexico, South Korea, European Union, France and Germany. The remaining written collaborative arrangements are between Customs Administrations.

3.13 Canada has also entered into Mutual Legal Assistance Treaties (MLATs) with 31 countries. It should be noted that MLATs govern the overall legal assistance in criminal matters between countries. Therefore they are not per se the sole responsibility of the CBSA; they are managed jointly with the Department of Foreign Affairs and International Trade and Justice Canada.

3.14 The officials authorized to approve the release of customs information under the relevant authorities of section 107 of the *Customs Act* are identified in CBSA policy and guidelines.

Certain agreements governing the sharing of information between Canada and the United States could be strengthened to provide stronger data protection safeguards.

3.15 The existing CMAA and MLAT between Canada and the United States are longstanding. In our view, they need to be updated. More important than the fact that they refer to customs agencies that no longer exist is that these agreements do not adequately address the management of personal information. This view is reinforced through an examination of CMAAs with other countries that do contain enhanced safeguards for protecting data. However, even these agreements, while more acceptable, could be improved.

3.16 The Agreement between Canada and the United States establishing mutual assistance and cooperation between their respective customs administrations was signed on June 20, 1984. The CMAA defines “customs administration” in Canada as the Department of National Revenue, Customs and Excise. The age of the agreement is evidenced by the fact that this department has been succeeded since by the Canada Customs and Revenue Agency (CCRA)

and, more recently, the CBSA. Similarly, the United States customs administration is defined as the United States Customs Service, Department of Treasury. The Customs Service is now largely part of the U.S. Customs and Border Protection Agency, within the Department of Homeland Security.

3.17 The existing CMAA between Canada and the United States stipulates that requests for information must be in writing and include:

- the identity of the authority making the request;
- the nature of the investigation;
- the names and addresses of the parties to whom the request relates;
- a description of the subject of the request and the legal issues involved; and
- the object of and reason for the request.

3.18 It should be noted that while requests for customs information must be in writing, there is an exception for urgent requests, i.e., where pressing circumstances exist. The agreement requires only that verbal requests for assistance be confirmed in writing at the request of the other party. The agreement also states that documents, information, and communications are to be kept confidential and granted the protection from disclosure under the laws of the receiving party. Further, the use of documents, information and communications for any purpose other than those contained in the agreement requires the prior written consent of the other customs administration.

3.19 As noted earlier, our audit included a comparison analysis of a number of CMAAs that Canada has entered with other countries. Using the CMAA between Canada and the European Union (EU) as an example, this agreement – which came into effect in 1997 – devotes more attention to personal information handling and generally provides better data protections than does the CMAA between Canada and the United States. Unlike the Canada-U.S. CMAA, the Canada-EU agreement provides that, while a verbal request may be made in certain circumstances, there is a requirement that such a request be confirmed in writing. The agreement between Canada and the EU also incorporates the “need-to-know” principle – that is, the dissemination of information among customs authorities with each country shall occur only on a need-to-know basis. The agreement also restricts communications regarding requests to specifically designated officials.

3.20 Further, Article 16 of the Canada-EU CMAA provides that shared information shall be treated as confidential. It also requires that information provided be subject to the same protection afforded by not only the laws of the receiving country, but also the laws of the country that provided the information. This means that information Canada provides to an EU country must be treated in accordance with both Canadian privacy laws and the laws of the particular EU country.

3.21 Similar to the CMAA between Canada and the U.S., the Canada-EU agreement also states the information cannot be used for purposes other than those specified in the agreement without prior consent. However, in addition, Article 16 further stipulates that such secondary use may be subject to any restrictions established by the country providing the information.

3.22 The Mutual Legal Assistance Treaty (MLAT) between Canada and the United States was signed in March 1985. Requests for assistance under the MLAT must include, among other things, the subject matter of the investigation, a description of and the purpose for which the information, evidence, and assistance is sought, and any requirements for confidentiality. Unless otherwise authorized by the requesting country, the responding country is required to use its "best efforts" to maintain the confidentiality of requests and their contents. The agreement also states a country may require information be kept confidential or that it be disclosed or used subject to certain restrictions. In addition, the requesting country is prohibited from using or disclosing information provided for purposes other than those contained in the request without prior consent.

3.23 Our audit included a review of other MLATs, including the MLAT between Canada and Germany of October 2004. When compared to the Canada-U.S. treaty, the Canada-Germany MLAT provides additional safeguards over any information that may be requested. These safeguards require that requests for information include:

- the identity of persons who are subject of investigation and, where possible, a list of questions and details of any right of that person to refuse to give evidence;
- a description of the alleged offence and a statement of the relevant law; and
- the subject matter on which individuals are to be examined.

3.24 The Canada-Germany MLAT also provides that the use of personal information shared by way of the treaty is limited to the purposes for which it is transmitted, to the prevention and prosecution of offences related to the treaty, to related civil court and administrative proceedings, and to avoid substantial public security threats. Any other use requires the prior consent of the country transmitting the information.

3.25 Under the same MLAT the receiving country must inform the transmitting country of any secondary use made of the information. Both parties must handle the information carefully and ensure that the information they provide is accurate and complete. If one party is aware that the information it has provided is inaccurate, it must advise the other country, which is then responsible for either correcting the information or returning it. The exchange of information is limited to that related to the request. Parties must maintain an appropriate record of the transmission and receipt of personal information and protect the information from unauthorized access, alteration, or disclosure.

3.26 Only one of the agreements that we reviewed requires that the processes for handling personal information be subject to audit. Auditing these processes would allow for reciprocal assurance between the two countries that the signatories are adhering to the terms and conditions of the agreements. The MOU for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information – signed in March 2005 – requires the participants to ensure that appropriate auditing and tracking mechanisms are in place to safeguard information. However, the MOU does not establish a requirement for the agencies to share the audit results with the other party to provide assurances that the obligations under the MOU are being met.

3.27 We believe the idea of reciprocal or mutual assurance regarding privacy to be important not only for information about Canadians that is shared with the U.S., but also for Americans whose personal information may be shared with Canada. A system of mutual assurance could include each country providing information to the other detailing the internal controls adopted in each jurisdiction for protecting personal information. The system could also require the parties to carry out internal privacy and security audits and share the results. These practices would allow each country to provide assurance to the other with respect to its regime for protecting data. They might also enable the parties to help each other follow sound data protection principles and practices.

Recommendation # 1:

It is recommended that the CBSA, as part of strengthening its privacy management framework, seek to update and strengthen its personal information sharing agreements with the United States, including the establishment of processes that provide mutual assurance that trans-bordered personal information is accorded appropriate protections.

CBSA Response:

In the near term, the CBSA will create a Privacy Management Framework to guide policy development and consider a plan to update existing Customs Mutual Assistance Agreements (CMAAs). CBSA will consider the elements of the Privacy Management Framework already in place and will work to clarify roles and responsibilities related to Privacy. We are developing guidelines on the development of written collaborative arrangements that reflect advice provided by the Office of the Privacy Commissioner (OPC). In the long term, guidelines will be revised to provide direction on the access, use and disclosure of personal information to foreign governments.

Written requests for assistance from foreign governments contain the required elements established under Customs Mutual Assistance Agreements (CMAAs) and the requests were processed in accordance with Section 107(8) of the Customs Act and CBSA policy.

3.28 The responsibility for responding to requests from other countries for assistance under CMAAs rests primarily with the CBSA's Enforcement Branch. Depending upon the nature of the assistance being sought, either the Customs Investigations Division or the Intelligence and Contraband Division process the request. With the exception of requests originating from the United States, all foreign requests for assistance under CMAAs are coordinated through CBSA Headquarters.

3.29 In November-December of 2003, the Canada Customs and Revenue Agency (CCRA) issued interim operational guidelines, Interim Memorandum D1-16-1 and D1-16-2. In addition to providing a clause-by-clause description of section 107 of the *Customs Act,* the guidelines provide direction for using customs information within the Agency. They also cover the disclosure of such information to external organizations, both domestic and foreign. The Memoranda supplement the information found in the CBSA's CMAAs and MLATs.

3.30 Memorandum D1-16-2 identifies the officials authorized to disclose customs information under the various clauses found in section 107 of the *Customs Act*. This Memorandum has not been modified since the CCRA created it, and the audit team was informed that its provisions remain in effect as CBSA operational policy.

3.31 As discovery or exploratory sampling, we examined 80 international assistance files. While our examination focused on the trans-border flow of personal information between the CBSA and the United States, it also included a sample of requests from other foreign governments. Our examination of the written request for assistance files confirmed that all of the information exchanges had been approved by officials who had the delegated authority under CBSA policy. We conclude that this basic aspect of internal control is working well.

3.32 The documentation contained in the sample established the authority under which the requests had been made, the nature of the investigation that the foreign customs agency was carrying out, and the exact nature of the disclosure. We are satisfied that the exchanges of information were permitted under the applicable CMAA, section 107(8) of the *Customs Act,* and that the disclosures made by the CBSA were limited to the information that was necessary to comply with the requests. The review also found no incidences in which the Agency had disclosed information from external databases – such as the Police Information Reporting System (PIRS) or the Canadian Police Information Centre (CPIC) – to a third party. We note that such information can be released only with the permission of the organization which controls that information.

The accountability framework and control environment surrounding verbal cross-border exchanges of personal information need to be strengthened.

3.33 Our audit examined the existing instruments – information sharing agreements and CBSA policies – that govern cross-border exchanges of personal information. Our observations relate to the level of compliance with the accountability framework contained in these instruments. It should be noted that our audit did not include assessing the relative merits of the requirements under the existing CMAA between Canada and the United States, including the requirement that exchanges of information be preceded by a written request unless urgent circumstances exist.

3.34 In general, our observations showed the following:

- In many instances, the CBSA has disclosed information to the U.S. without a written request from that country.
- Information is often disclosed without first obtaining approval from a designated CBSA official, which contravenes the Agency's policy.
- We found weaknesses in the record keeping associated with disclosures of information.

3.35 Regarding the release of information without a written request, we interviewed selected managers and regional intelligence officers (RIOs) within the Intelligence and Contraband Divisions that we visited. They told us that many exchanges of information with the U.S. occur at the regional level without a written request, contrary to the existing Canada-U.S. CMAA. Of the 22 RIOs whom we interviewed, approximately 64% or 14 acknowledged that they do share

customs information – including personal information – verbally with their U.S. counterparts. Of the eight RIOs who reported no involvement in cross-border verbal exchanges, six were from the same region. These officers explained that their specific role and area of concentration meant that they were not involved in verbal exchanges with U.S. authorities. During follow-up meetings with three managers of this region, the audit team was informed that RIOs may share information with the U.S. One manager described daily exchanges between some RIOs and the U.S. as being verbal in nature 80 to 95% of the time.

3.36 The frequency of verbal contact with the U.S. varied among the 14 RIOs who reported involvement in cross-border exchanges of information, and was dependent in large part upon their specific role and location. While the estimates varied, approximately one-half of the respondents indicated that verbal disclosures represented between 70-90% of their exchanges with U.S. customs authorities, and could include the following information:

- an individual's passage or travel history;
- a general synopsis of previous enforcement actions;
- confirmation of the existence of a file held by the CBSA;
- confirmation of the existence of a file with another law enforcement agency.

3.37 In terms of the extent of verbal sharing, the audit team was informed that an exchange would not occur if it could either potentially compromise ongoing investigative and intelligence activities, identify a confidential source of information, or reveal information that an external organization (third party) had supplied to the CBSA.

3.38 With one exception, the RIOs reported that a written request would be required prior to releasing documentation to the U.S. Using the example of a previous enforcement action, the audit team was informed that while general details surrounding a customs seizure might be shared verbally (the exception being seizures involving currency), a written request would be required if the U.S. wished to obtain a copy of the seizure report and supporting documentation.

3.39 We also interviewed 10 customs inspectors and four customs superintendents at the land border crossings that we visited. Of these, 6 of the 10 inspectors and two of the four superintendents indicated that they have (although rarely) shared the results of name and vehicle queries with U.S. border protection officers. We note that vehicle crossing information represented the majority of such disclosures. In terms of airport operations, we interviewed eight customs inspectors and three superintendents. None reported involvement in exchanges of information with the U.S. It was explained that requests for assistance originating from the U.S. are referred to the RIO on site.

3.40 With respect to the process for approving requests for information, under its D-1-16-1 and D-1-16-2 Memoranda, the CBSA has identified and designated specific officials with the authority to approve disclosures of information under the various provisions of section 107 of the *Customs Act*. This policy requires that a designated official must authorize the release of information to a third party. The exception is if urgent or imminent circumstances exist (e.g., the release of information is necessary to protect life, health or safety of an individual) and prior approval cannot be obtained. All such exceptions are to be reported to a designated official as soon as possible after the event.

3.41 At the regional level, the authority to release customs information to foreign governments has been delegated to the Manager/Director of a customs program area. The audit found a low level of compliance with the policy. In many instances, information is shared verbally with U.S. customs officials without prior approval. Although there were exceptions, the RIOs involved in exchanges with the U.S. generally acknowledged that verbal exchanges – disclosures in response to a U.S. request for assistance and ongoing exchanges that relate to files of common interest – occur without prior approval from the Manager/Director. Similarly, the customs inspectors who reported sharing information with their U.S. counterparts conceded that such exchanges take place without obtaining prior authorization from a manager.

3.42 In our view, a lack of compliance with the policy undermines both the Agency's overall control and accountability framework, and its ability to effectively monitor its information sharing practices with foreign entities to ensure that they comply with the requirements of the *Customs Act* and the *Privacy Act*.

3.43 As noted above, we found weaknesses in the record keeping relating to releases of personal information. An individual's right to privacy includes the right to know what personal information government institutions collect, under what circumstances this information may be shared with a third party, and with whom it will be shared. In fulfilling this obligation, it is essential that institutions create and retain records relating to all disclosures made to external organizations.

3.44 Under CBSA policy, officials must retain records of all customs information requested and released to external organizations. Records include the name of the requester, the date the request was received, the purpose for which customs information is required, the nature of the information disclosed and the rationale for the decision taken. The audit found that compliance with this policy is lacking. Of the 14 RIOs who confirmed their involvement in verbal exchanges with the U.S., fewer than 50% record such disclosures in all cases.

3.45 The audit team found that where a file on a U.S. request for information exists in the CBSA's Intelligence Management System (IMS), a notation of the verbal disclosure is generally captured in the system. However, the administrative action taken with respect to other verbal exchanges of personal information where no corresponding IMS file exists varied among the respondents. Some indicated that the verbal exchange would be recorded in their notebook or on a Provision-Access and Use of Customs Information Report (CBSA Form E675). Others responded that the decision to record would depend upon the type of information that was provided. Name checks, traveller passage queries and general seizure information were cited as examples of the type of exchange that would not be recorded. The remaining RIOs reported that no record of the verbal exchange would be retained.

3.46 Regarding the land border crossings that we visited, five of the six customs inspectors who have shared the results of name and/or lane checks with the U.S. reported that these disclosures are not generally documented. In summary, our audit found that verbal disclosures of personal information to the U.S. are not being recorded on a consistent basis.

3.47 The level of detail in which verbal exchanges are reported in the Intelligence Management System (IMS) and officer notebooks is an area requiring attention. The audit indicated that the IMS or notebook entries did not always record the name of the official requesting the information, the purpose for which the information was requested or the exact nature of the disclosure, i.e., the specific information that was released in response to the request.

3.48 It should be noted that our observations relating to records of verbal exchanges of information are based on the limited sampling of notebook and IMS entries that CBSA provided for our examination. Given the size of the sample, we cannot say whether a pervasive, systematic problem exists. However, our audit work did provide a strong indication that the manner in which exchanges are recorded needs improvement. Without adequate reporting, the CBSA cannot objectively assess whether its trans-border information sharing activities respect individual privacy rights.

3. 49 We have concluded that without proper record keeping, it is not possible for the CBSA to either fully measure the extent to which information sharing occurs, or assess whether it is appropriate in all cases. Moreover, in the absence of records, individuals cannot exercise their right of access to personal information under section 12(1) of the *Privacy Act*.

Recommendation # 2:

It is recommended that the CBSA formulate an action plan to address verbal exchanges of personal information. Such a plan should consider:

- *determining the extent to which customs information is being shared verbally with United States customs authorities and implement measures to ensure that all disclosures consistently comply with governing agreements and policies;*
- *implementing measures to ensure that all disclosures of personal information are recorded as required under CBSA policy;*
- *issuing a communiqué to all staff regarding the approval process governing disclosures under subsection 107(8) of the Customs Act, and reinforce the policy requirements by including a specific module in the delivery of Section 107 and Privacy Act training sessions; and*
- *monitoring compliance with policies governing cross-border exchanges of data to ensure that adequate management controls are in place to protect personal information from unauthorized disclosure.*

CBSA Response:

CBSA agrees with the recommendation and will create an action plan to review our existing practices and guidelines concerning the use, access to and disclosure of customs information. We will create standards and tools for reporting disclosure activity that will reflect both operational requirements and recommended practices articulated by the Privacy Commissioner. The CBSA supports the new guidelines with targeted training and awareness seminars and will monitor the implementation of the revised direction. Further, we will review relevant training materials for the POERT (former CIRTP) training programs to ensure new staff understand Privacy related requirements related to the use, access to and disclosure of customs information. We will work to enhance our capacity to monitor the compliance of the guidelines.

The CBSA cannot, with a reasonable degree of certainty, report either on the extent to which it shares personal information with the United States, or how much and how often it does so. Furthermore, the CBSA cannot be certain that all of its information sharing activity is permitted under section 107 of the Customs Act and Section 8 of the Privacy Act.

3.50 To assess the extent to which its information sharing activities with the United States comply with the *Privacy Act,* the *Customs Act* and the bilateral agreements between the two countries, the CBSA must have the capacity to track all trans-border exchanges of personal information. This capacity is significantly underdeveloped at the present time.

3.51 One of the objectives of this audit was to report and map, to the extent practical, what information about Canadians the CBSA transmits to the United States, how this is done and for what purposes. Initial inquiries were directed at establishing what reference material the CBSA had that would assist in this regard, including data-flow diagrams and program descriptions. In addition to providing records outlining the automated exchange of lookouts and advance passenger information, the CBSA provided a chart that captured, in general terms, the information sharing process – that is, the legal authority for sharing, name of the international agreement, the type of information shared (e.g., information required to enforce customs laws) and the mode of transmission (written or electronic).

3.52 While the task of mapping data flows for the shared lookout and HRTI initiatives can be accomplished with relative ease, such is not the case for the other ongoing exchanges between Canadian and U.S. customs authorities at the regional level.

3.53 As reported earlier, a number of these disclosures are verbal and unrecorded. Further, we found that documentation of verbal disclosures is dispersed among various locations such as officers' notebooks and electronic files and are not easily identified as retaining information that has been exchanged across the Canada-U.S. border. This situation prevented us from using a random sample approach in conducting file reviews. Instead, as noted previously, the audit team had to rely upon CBSA personnel to identify files for examination, more or less from their recollection of specific cases. Once identified, the notations relating to verbal exchanges in a number of these files did not clearly indicate what information had been sent across the border and for what specific purpose.

3.54 Without a corporate mechanism for recording all details of the Agency's trans-border data flows of personal information, the CBSA has limited ability to measure its level of compliance with the legislative and policy framework governing the sharing of information with foreign governments or their institutions. Moreover, CBSA management cannot obtain a full accounting of what personal information is being exchanged and the extent of the exchanges. Furthermore, management cannot provide this information to others – such as Parliament, the Privacy Commissioner and the Canadian public.

Recommendation # 3:

It is recommended that the CBSA implement ways and means of capturing all trans-border data exchanges for program management and accountability purposes. This might include – but is not limited to – the construction of data-flow diagrams, modifications to existing information systems to reliably record and identify all sharing activities with foreign governments.

CBSA Response:

CBSA agrees with the recommendation, and acknowledges that we will need to further document preferred disclosure practices. This work can form part of the plan to strengthen our planned Privacy Management Framework. We will consider guidelines to strengthen procedures designed to document disclosure and ensure appropriate management accountability for the compliance with guidelines on the use, access to and disclosure of customs information. We will work to ensure all Branches and Regions are familiar with revised guidelines and preferred processes. Our intention is that the guidelines will reflect both the terms and conditions of our legislative authority and also reflective of generally accepted privacy principles.

Additionally, such trans-border data exchanges will be identified and described in narrative and diagrammatical documentation, and system audit trails will be incorporated into IT systems to identify and log sharing activities with foreign governments.

The CBSA audit trail strategy is currently under development and the framework will be completed by December 2006 in order to ensure required audit trails and log sharing activities are part of our Software Development Lifecycle (SDLC) for projects and systems.

INTEGRATED CUSTOMS ENFORCEMENT SYSTEM (ICES)

Background

3.55 Government departments and agencies largely depend on information databases, programs, and networks to carry out their respective mandates. As the personal information under the CBSA's control resides primarily in electronic databases, our audit included reviewing and assessing the controls of key IT systems. These controls are critical to ensuring that personal information is adequately protected. Vulnerable data make not only for poor security but also poor privacy.

3.56 The Integrated Customs Enforcement System (ICES) is an automated customs enforcement support system. Under the terms of a MOU, the CBSA acquires its informatics services infrastructure from the Canada Revenue Agency (CRA). This agreement extends the terms of a service arrangement that existed when the customs and revenue programs were both part of the former Canada Customs and Revenue Agency (CCRA). The CBSA is responsible for all internal security controls of the ICES.

3.57 The ICES database is designed to support the functions of front-line customs inspectors, intelligence and investigations personnel by allowing them to collect, analyze and disseminate information related to risks at the border. It also provides a common repository for customs enforcement data, e.g., data on arrests, seizures and ongoing customs investigations.

3.58 Customs inspectors and intelligence officers are able to create access, maintain and disseminate lookouts (see text box below) at the local, regional, and national level. The Primary Automated Lookout System (PALS) at land border crossings (licence plate reader) and the Integrated Primary Inspection Line System (IPIL) at airports (travel document reader) will return lookout, caution and enforcement data-match hits from the ICES database to customs inspectors. The system's operational reports provide transaction level details on lookouts, seizures and passage history of individuals and conveyances at borders and airports.

A "lookout" is an electronic file record created in the ICES. The lookout flags or identifies particular travellers or vehicles according to various risk indicators or other available intelligence.

Personal information

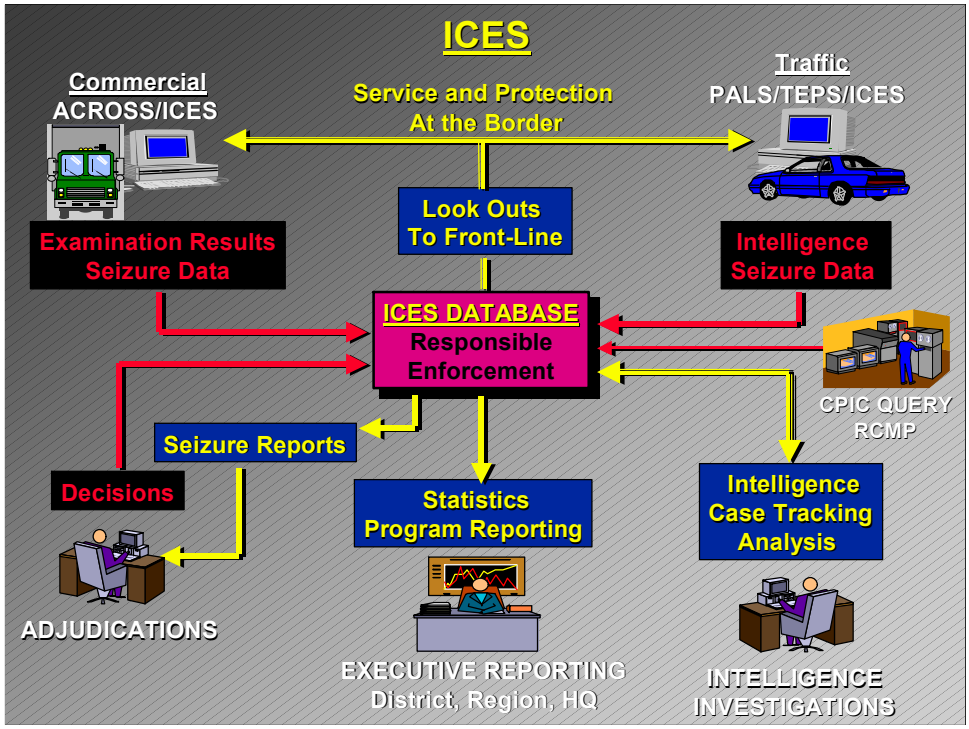
3.59 All information pertaining to an enforcement action taken against an individual or business is entered into the ICES database. The personal information retained therein would typically include, among other things:

- the reason(s) the individual was referred to secondary screening;
- the results of the search and notes of interviews conducted during the secondary examination;
- tombstone data – name, age, address, citizenship, licence number, passport number;
- the enforcement actions taken (individual was searched, arrested, detained, etc.) and the results of the inquiry;
- the identity of travel companions.

3.60 Other details related to conveyances, commodities, methods of concealment and indicators are also reported. Customs inspectors can automatically receive information on an individual through an automated previous offender query that captures previous seizures or customs warnings associated with a given person.

Flow of Personal Information

Source: CBSA description of the Integrated Customs Enforcement System (ICES) – January 21, 2005



Notes:

With the exception of the Canadian Police Information Centre (CPIC) databank, all programs indicated above are under the control of the CBSA.

Traffic refers primarily to non-commercial travellers, which was the focus of the audit. While not reflected in the above diagram, the traffic icon also includes the IPIL system – utilized to process air travellers arriving in Canada.

Adjudications refers to appeals from administrative decisions under the *Customs Act,* an area that was not examined as part of this audit.

Disclosures to foreign governments

3.61 As described elsewhere in this report, personal information collected by the CBSA may be released to foreign governments or agencies under Mutual Legal Assistance Treaties (MLATs), Customs Mutual Assistance Agreements (CMAAs), Memoranda of Understanding (MOUs) or other agreements and arrangements. Section 107(8) of the *Customs Act* provides the legislative authority for such disclosures.

3.62 On March 9, 2005, the CBSA and the U.S. Customs and Border Protection Agency signed a MOU to facilitate the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information (API). The National Risk Assessment Centre (NRAC) – examined as part of this audit – and the U.S. National Targeting Centre (NTC) jointly manage the initiative.

3.63 When intelligence officers, intelligence analysts and other authorized CBSA employees create a lookout, they have the option of sharing the lookout with the United States. If a lookout is selected for sharing, it is forwarded electronically to the NRAC for review. After confirming that the lookout meets the criteria for sharing, it is transmitted electronically from the ICES application to the U.S. Treasury Enforcement Communications System (TECS). Once this transmission has been completed, the lookout is accessible to U.S. customs authorities at ports of entry.

3.64 Our review evaluated the controls in place to safeguard the integrity of personal information that the CBSA manages within the ICES shared lookout program. The IT review of controls over the ICES database relate directly to the CBSA's obligations under sections 4 to 8 of the *Privacy Act*. The audit focused on the privacy and security protections for the use, disclosure and integrity of lookout data stored within the CBSA IT infrastructure, as well as the transmission of shared lookout data between the CBSA and the U.S. We also reviewed the logical and physical security over personal information, IT change management, and operations IT controls. The audit team considered the following ICES activities during the examination:

- cross-border exchange of shared lookouts; and
- specific IT security controls for the ICES.

3.65 Our IT audit of the ICES database was conducted in tandem with the audit examination of the National Risk Assessment Centre's shared lookout and HRTI initiatives. It should be noted that our audit did not include an evaluation of the IT control environment utilized by the U.S. NTC to protect information once the CBSA has transmitted it to the U.S.

The Integrated Customs Enforcement System (ICES) Security Architecture is well designed.

3.66 The architecture of the system refers to the mainframe computer and servers as well as all communication links, firewalls and defined security zones intended primarily to protect the system and its contents from external attacks. Well defined and constructed IT architecture provides the foundation for other security and privacy-enhancing IT controls.

3.67 We found that the security architecture surrounding the ICES application and systems is well designed. It provides several types of protection at every critical IT level and a central control over access between controlled zones.

3.68 The MOU between Canada and the U.S. covering the exchange of lookout information requires the CBSA and U.S. Customs and Border Protection to respect each other's expiration, cancellation and modifications to lookouts. However, the MOU contains few details about the specific IT controls that are used to protect personal information within the U.S. Treasury Enforcement Communications System (TECS). As noted above, our audit did not evaluate the controls for protecting this information once it has been transmitted to the U.S. However, we see opportunities for improving the bilateral control framework.

Recommendation # 4:

It is recommended that the CBSA work with its U.S. counterparts to provide mutual levels of assurance that respective IT security controls are adequate to protect the privacy of citizen data in shared lookouts. In this regard, specific consideration could be given to extending Service Level Agreements to include descriptions of the processes to delete shared data upon expiry or cancellation, and the requirement for regular privacy and security audits.

CBSA Response:

The responsibility of our U.S. counterparts to protect the privacy of citizen data in the shared lookouts is integral to the MOU signed between the CBSA and the United States Customs and Border Protection (USCBP) for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information (API). The U.S. has also put in place a process for the deletion of expired and/or cancelled lookouts.

A review of the current SLA's will be undertaken and improvements will be made to the bilateral control framework by December 2006.

United States customs authorities do not have direct access to the ICES.

3.69 Our audit confirmed that the ICES application does not permit U.S. authorities to access personal information directly. Electronic communications between Canada and the U.S. are performed as a "push" rather than a "pull", with the CBSA providing selected lookout information to the U.S. after the CBSA has verified that the information can be shared.

3.70 The exchanges between the ICES and TECS systems are encrypted with approved algorithms using hardware cryptographic devices to protect data integrity in transit. Failure of these devices is monitored.

Printing of lookout data is not logged.

3.71 User logs are IT reports about users' activities in a particular system. They are retained in the system and can be printed for verification purposes. These logs include user IDs and computer identification, as well as file numbers that have been accessed, modified or deleted with date and time. Logs are important audit tools for tracing the activities of individual users on an ongoing or ad hoc basis. Logging these activities is key to determining whether access rights have been appropriately exercised according to the need-to-know principle. User logs –

and their use as a tool for monitoring and auditing purposes – are necessary to ensure the integrity of program information and to ensure that use and disclosure of the information is in compliance with privacy principles and organizational policies. However, users (employees) should be informed, through notices and security policies, that these control procedures exist. Access to such logs must be strictly controlled to prevent inappropriate use and disclosure.

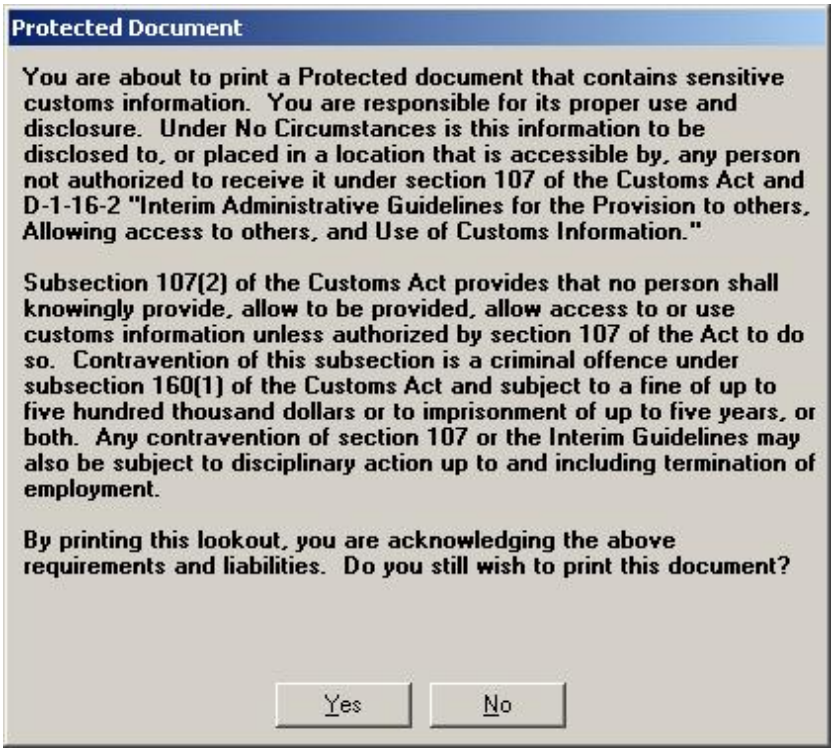
3.72 While the ICES logs all activities conducted with the application, it does not log the printing of lookout data that may contain personal information. This presents a possible avenue for disclosure of personal information, either through accident or malicious intent, without an audit trail or history to track and identify the source of the disclosure back to an individual user.

Recommendation # 5:

It is recommended that the CBSA modify the ICES application to ensure that the logging capacity includes when an ICES printout is made.

CBSA Response:

At the present time the following message appears before any lookout is printed in ICES



In addition to the print warning provided, all CBSA systems include a general warning at the time of log on that the use of systems is for authorized users and official business.

Required information will be incorporated into ICES audit trail as part of the CBSA audit trail strategy and implemented into the ICES system by December 2006.

The CBSA's IT Change Management Framework is well defined.

3.73 Change management in the IT context is a systematic approach to adapting to, controlling and introducing changes to a particular IT system, so an organization can address any new operational requirements of that system. Change management relies on developing procedures, controls, technology and software to modify IT hardware and software programs. Effective change management is essential to preserving an organization's data assets, improving program delivery and protecting the integrity of personal information used for its decision-making processes.

3.74 The audit found that the CBSA – along with the CRA – had a well defined and controlled change management framework and process for designing, developing and testing new IT requirements. This process follows an approved industry standard process for incorporating IT changes, including:

- changes and upgrades to application functionality;
- database changes and upgrades;
- changes to transaction volumes; and
- operating system patches.

3.75 The change management testing process allows for the safe testing of a migration plan for the anticipated changes in a separate test environment, without risk of negatively affecting the current operating system/program or the integrity of its information holdings.

3.76 The CBSA's team approach to change management provides a broader skill set and better checks and balances to ensure the integrity of changes and program code than if one person were responsible for such major changes. This approach also helps to mitigate the risk of accidental or malicious IT changes or the insertion of "backdoors" into programming code that could affect the confidentiality and integrity of data processed and stored by the ICES application. As an added precaution, the CBSA does not allow IT program developers to have access to the final production environment.

3.77 The CRA requires all changes to the ICES environments to pass through a 22-person committee, which meets on a weekly basis. Any change requires five signatures before it can be implemented. When changes are required to the data in the ICES database, a process of authorizations is followed and changes are logged.

3.78 Our inquiries did identify a number of minor issues for CBSA's consideration. Specifically, three Database Administrators in the CBSA have the privileges to make ICES database changes. New database staff must be trained and must demonstrate their ability to perform changes before being given any dBA access. We noted only one instance during a database change where back-out procedures were not followed because they were technically not possible.

3.79 We also noted that the CBSA lacks documented procedures for removing a server from production and pre-production environments and providing appropriate controls over confidentiality and integrity of data on the server. Again, only one instance of this situation had been noted and appropriate steps were taken to safeguard the assets.

IT roles and responsibilities need to be clearly defined.

3.80 It is important that various IT roles and responsibilities be clearly described and communicated to all parties. Clarity in this area is central to effectively managing the many IT security controls required to protect customs and personal information across organizations (CBSA and CRA), programs and geographic areas. This task would include defining leadership roles (i.e., of the Departmental Security Officer and Information Technology Security Officer) as well as functional IT managers, specialists and users.

3.81 At the time of the audit, the CBSA lacked updated organizational charts and contact lists to document roles and responsibilities under its new IT security framework. This is an underlying problem with a number of the IT control categories and reflects the CBSA's fairly recent creation as an independent organization.

3.82 Our audit found that security roles within the CBSA are highly distributed to support the specific needs of each program and application. The risk of this decentralized control structure is that there may be inconsistency in the way each program area complies with common standards, policies and training requirements. Any major divergence from baseline standards may create a weak link in the Agency's security chain. Any weakness in the chain could lead to security breaches and compromise personal information.

3.83 We note that the CBSA and the CRA have signed Memoranda of Understanding and Service Level Agreements that define the roles and levels of service expectations – including security expectations – between the organizations.

Recommendation # 6:

It is recommended that the CBSA establish and communicate the roles and responsibilities of all designated IT officials in the organization, including updating job descriptions and organizational charts.

CBSA Response:

CBSA is currently reviewing and clarifying the IT roles and responsibilities. Significant progress has already been made in clarifying and defining the roles and responsibilities with respect to IT Security and the DSO. These responsibilities are also aligned with the TBS operational standard for MITS, including the governance and structure of organizations. Clarified roles and responsibilities will be in place and communicated by December 2006.

The CBSA is creating a security management framework.

3.84 The CBSA created the Departmental Security Officer (DSO) role and organization in 2004. The DSO has been recently charged with developing and implementing a cohesive security management framework for coordinating all aspects of security throughout the Agency.

3.85 This framework should provide the necessary tools, methods and structures for implementing a security network from one program area to another, covering all aspects of security for the CBSA, including informational security and privacy. It should also provide the Agency with a stronger basis for ensuring that no one area of security control becomes the weak link that could undermine the organization's entire security framework. In our view, a key component of the framework would be an evaluation to assess the effectiveness of the framework in protecting personal information.

Recommendation # 7:

It is recommended that the CBSA continue its efforts to create a cohesive security management framework. It should audit this framework within a year of its implementation to ensure that it is operating efficiently to protect customs and personal information. We also request that the CBSA provide the results of this audit to the Office of the Privacy Commissioner of Canada.

CBSA Response:

The CBSA intends to have a complete security management framework implemented by the end of fiscal 2007. The feasibility of an audit or post-implementation review will be considered at that time. Privacy related results arising from an audit or review conducted on the security management framework will be shared with the Office of the Privacy Commissioner.

Access rights to the ICES are in keeping with the need-to-know principle.

3.86 Controlled access rights to an IT system and its various data elements represent a key safeguard because they restrict the use and disclosure of personal information to those individuals with a legitimate need. An effective method of mitigating the risk of inappropriate use and disclosure of personal information is to limit access rights to the system to a small number of users.

3.87 The creation of new ICES user profiles is tightly controlled through processes within the operational units and the IT Help Desk. Only those with a need-to-know receive access to ICES information, and only at the level necessary for their job position and defined functions.

3.88 The creation of user profiles is supported through a user account request form that must be signed by the user and authorized by the individual's manager. By signing the user request form, the individual accepts responsibility for maintaining the confidentiality of the data. A recent change also requires users to acknowledge that they should not share their user profile or password. The level of access required by the user is assigned and verified by the individual's manager before being sent to the IT Help Desk, where a user profile is created and the individual's access rights are activated.

3.89 We were advised that new users receive some security awareness training from their respective program managers. This training emphasizes the need to maintain the confidentiality of information obtained from the ICES database. It also covers procedures for managing accounts/passwords to prevent non-users from obtaining access to the system.

3.90 To help manage user profiles and accounts in general, a recent CRA project was implemented to continually review the need for Privileged User Risk Management System (PURM) accounts in the CRA and the CBSA. The purpose of the project is to improve both the integrity of user account assignments and password strength/management commensurate with the users' roles. The use of effective password management policies ensures that passwords are changed frequently, are not reused and are so constructed as to avoid detection. Recent upgrades to the proprietary Active Directory System within the CBSA and CRA will also assist in properly managing user accounts at the organizational level.

3.91 Although access to the ICES database is generally well controlled, the process for requesting audit trail information was, until recently, maintained by the same officials who reviewed the audit trails. The CBSA has taken corrective action to remedy this situation and has assigned the responsibilities for maintaining and monitoring audit trails to separate individuals. We also noted that at the time of the audit, the ICES database manager accounts were not monitored or audited.

Recommendation # 8:

It is recommended that the CBSA log and monitor database administrators' access to and the operations performed on the ICES database.

CBSA Response:

CBSA has reviewed the procedures and processes for logging and monitoring the ICES database administrator's access and implemented additional control measures. The CBSA's audit trail strategy will further improve audit capabilities on the ICES system by December 2006.

PASSENGER INFORMATION SYSTEM (PAXIS)

Background

3.92 The Passenger Information System (PAXIS) is a data bank, application and IT system that the CBSA uses to support its risk management strategy for screening millions of air travellers entering Canada annually. It was developed and implemented in 2002-03 to manage advance passenger information/passenger name record (API/PNR) data – see text box under "Personal information", below – that it receives from airlines, travel agents and automated ticket systems. The CBSA has announced plans to extend the use of the PAXIS application to other modes of transportation in the future.

3.93 The legal authority for collecting API/PNR information is derived from the *Customs Act* and the *Immigration and Refugee Protection Act* and *Regulations.* The CCRA's *Passenger Information (Customs) Regulations* prescribe that commercial carriers and charters, travel agents, and owners and operators of a reservation system are required to provide the Minister of National Revenue (now CBSA) with, or provide access to, specified personal information on all passengers and crew members en route to Canada at the time of the commercial conveyance's departure.

3.94 The CBSA uses the PAXIS data bank to store API/PNR data on passengers and crew on international flights destined for Canada, before they arrive here. The system facilitates automated queries between API received from airline departure systems, with information retained on CBSA and Citizenship and Immigration Canada enforcement databanks – e.g., previous customs infractions and individuals who are the subject of a criminal or immigration warrant.

3.95 The PAXIS application facilitates the matching of API and PNR data on some or all passengers on selected flights for further risk analysis by the CBSA's Passenger Targeting Units (PTUs). These units are located at eight airports in Canada. PNR information is validated by the PTUs against various enforcement and intelligence sources to assess the risk posed by selected travellers. Based on this assessment, an electronic "lookout" may be created, which generally results in the traveller undergoing a secondary examination.

3.96 The data acquisition system (DAS) for API/PNR information is the iDetect messaging software tool provided by a third party, the Société Internationale de Transport Aéronautique (SITA), under contract with the CCRA (now CBSA). This tool continues to reside on the Canada Revenue Agency's IT network. SITA is also responsible for providing the secure transmission of traveller data from airlines and travel agents to the PAXIS data bank.

3.97 The CBSA began to collect API electronically from the first group of airlines on October 7, 2002. By the end of January 2003, the Agency was receiving API data from about 70% of air carriers. The CBSA indicated that 100% of commercial carriers currently provide API data. We noted, however, that the Agency does not always receive all API data elements for every flight.

3.98 The Agency began to collect PNR information from air carriers on July 8, 2003. The quantity and quality of PNR data that the CBSA receives remains problematic. In response to data quality issues identified in the post-implementation review of the PAXIS application, a data analysis function was established to monitor and analyse these problems. The CBSA continues to work with individual airlines to develop and implement solutions.

Personal information

3.99 API/PNR information consists of various data elements as shown in the text box. All travellers and crew members arriving in Canada by commercial air carriers are affected by this initiative.

API/PNR DATA ELEMENTS

Advance Passenger Information (API)

API is contained within the machine-readable zone (MRZ) portion of a passenger's or a crew member's travel documents (e.g., passport, permanent resident card). The API data elements include the individual's full name, date of birth, gender, citizenship or nationality and travel document number. The API that appears in the PAXIS database does not include citizenship and nationality. It does, however, include the travel document's country of origin.

Passenger Name Record (PNR)

PNR information includes personal data related to the traveller's reservation and travel itinerary as contained in a commercial carrier's reservation system. The specific data elements are listed below:

PNR locator code	Travel agency	Seat information
Date of reservation	Travel agent	One-way tickets
Dates of intended travel	Split/divided PNR information	Any collected API
Passenger Name	Ticketing information	Standby
Other names on PNR	Ticket number	Check-in information
All forms of payment information	Seat number	
Billing Address	Date of ticket issuance	
Contact telephone numbers	No show information	
All travel itinerary for specific PNR	Bag tag numbers (baggage information)	
Frequent flyer information	Go show information	

Flow of personal information

3.100 The following steps illustrate the flow of personal information for passengers on a typical international flight to Canada.

- A traveller books a flight to Canada through a travel agent, a representative, an airline, or directly through a web-based booking system.

- The booking agent obtains relevant information and creates a Passenger Name Record (PNR) based on the information provided by the passenger.
- The PNR is transferred from the booking agent to the airline's Departure Control System (DCS).
- When the traveller checks in, the airline counter agent captures the Advance Passenger Information (API) data along with the baggage and seat assignment and issues a boarding pass.
- The updated data elements are entered into the traveller's existing record in the DCS.
- After the aircraft has departed, the airline DCS transmits the API and PNR data to the PAXIS database in the CBSA.
- The API/PNR data received by the CBSA is verified against enforcement and intelligence database information and is risk scored to determine whether the traveller should be subjected to further review.
- If the traveller is identified for further review, a lookout is issued in the ICES and linked to the Integrated Primary Inspection Line (IPIL) system used by front-line customs inspectors at airports.
- Upon arrival at the primary inspection line, the individual's travel document (passport) is scanned on the IPIL card reader or the information is entered into the system manually by the customs inspector.
- The IPIL system queries customs and immigration databases for lookouts and if a match is detected, the traveller is referred for secondary screening.
- Where the subject of a lookout is intercepted, the results of the secondary screening process are communicated to the officer who issued the lookout by way of an electronic note or inspection report.
- We would also note that irrespective of individuals who are the subject of lookout notices, other travellers may be referred for secondary screening, with the primary customs inspector having discretion in this regard. Referrals may also be made on a random basis.

Releasing information to foreign governments

3.101 The legal basis for sharing API/PNR data is provided for under the commitments advanced by Canada and the United States under the Smart Border Declaration and 30-Point Action Plan, section 107 of the *Customs Act*, the *Immigration and Refugee Protection Act (IRPA) Regulations* and the MOU for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information.

3.102 The audit found the following IT controls for the PAXIS database to be adequate:

- The management and security of the data link between Canada and the U.S.;
- access to CRA data centres and offices housing PAXIS information;
- data management within PAXIS;
- the controls surrounding account set up; and
- comprehensive technical documentation of PAXIS.

No formalized service level agreement exists between the U.S. and Canada covering security and the accuracy of data.

3.103 Through interviews conducted with CBSA IT staff and management, we found that although a MOU is in place that outlines the sharing of information between Canada and the United States, there is no formalized service level agreement between the two countries that:

- specifies common security standards;
- defines an acceptable level of data accuracy; and
- indicates who is responsible for the accuracy of data shared between partners.

3.104 If standards of security are not defined, implemented and reviewed, they may not be adequate to protect the personal information of either Canadians or travellers from other countries. Again, as noted above, if responsibilities and standards for ensuring an acceptable level of data accuracy for personal information shared between partners are not defined, there is a risk that inaccurate data could lead to administrative actions that could negatively affect individual travellers.

Recommendation # 9:

It is recommended that a formal service level agreement be implemented between the U.S. and Canada to include mutually agreed security standards (based on the Government of Canada MITS security standard and standards on data quality and screening) so that each party takes steps to ensure that shared personal information is complete, current and accurate.

CBSA Response:

The CBSA currently reviews data prior to disclosing it to the U.S. to ensure that it relates to the traveller pending arrival and that it is applicable to privacy, third party and other legislative requirements as well as program requirements.

CBSA will work with their U.S. counterparts to establish comprehensive service level agreements that address the application of sufficient security standards on all personal information shared between the two countries.

In addition, CBSA is implementing a risk management framework that will address the need to regularly review potential vulnerabilities to the confidentiality, integrity, and availability of such information.

Individual access rights to the PAXIS data bank have not been reviewed and validated frequently enough to ensure that they remained valid.

3.105 Managing access rights for IT systems requires good coordination and communications between users, their managers, IT and Human Resources personnel.

3.106 The CBSA has an IT policy that calls for carrying out reviews of individual access rights on a quarterly basis. Our audit found, however, that the review and validation of access listings within the PAXIS data bank had not been done on a regular basis over the past two years. Documents that we examined during the audit showed that the Agency had performed a review in April 2005, and an earlier one 10 months prior in June 2004. We shared these observations with the CBSA. Since then, the CBSA performed a more recent review, the results of which were provided to us in September 2005.

3.107 We also noted that the roles and responsibilities related to the PAXIS support desk, as outlined within the PAXIS Support Desk Document version 3.0, do not include guidelines for revoking users' access to the system.

3.108 We looked at a sample of user accounts and compared them against human resource records on the individuals. Although many accounts had been deleted in the latest quarterly review, some had not been deleted one year after users had left the CBSA.

3.109 Without a clearly defined process for administering access rights across the organization, including regular reviews of access listings and procedures to remove user access rights as soon as an individual's job/position/role changes, there is increased risk that some access rights will not reflect the current roles and responsibilities of the system's users. There is also an increased risk of unauthorized access when accounts are not deactivated after the user account is no longer required.

3.110 A checklist should be consistently followed in all cases, and could be triggered by any of the following events: an access review; managers identifying a change in the role or employment status of one of their employees; human resources officials identifying a change in an employee's role or responsibilities due to a change in job classification; PAXIS support team identifying a change in role/responsibilities due to a request for additional access; and the production of quarterly reports of access to ensure accuracy of access rights based on the need-to-know principle.

Recommendation # 10:

It is recommended that a standard system rights checklist be used when a change in an employee's roles, responsibilities or employment status requires his or her manager to evaluate what system access rights the employee needs, what new system access permissions are required, and what permissions should be revoked.

Recommendation # 11:

It is recommended that the PAXIS Support Desk Document be updated to include guidelines for revoking system access rights. We also recommend that CBSA Human Resources refer to the checklist to ensure that employees who change positions, those on long-term leave and individuals who have left the organization have had their system access rights reviewed and revised or deleted accordingly.

CBSA Response to Recommendations # 10 and # 11:

CBSA will review current processes and procedures with respect to system access rights and permissions and develop a checklist to be used when there is any change in employee status. The implementation of the Privileged User Risk Management (PURM) System will also assist in improving the overall integrity of user account assignment and passwords.

Audit log monitoring of viewing, retrieval and modification of the PAXIS server or database related information by systems administrators is not performed.

3.111 Through interviewing key IT staff from the CBSA data management team and the CRA Infrastructure group, we found that, even though audit log information is available and can be retrieved, the CBSA does not actively monitor the access of database administrators or server administrators within the PAXIS.

3.112 The absence of active monitoring of the PAXIS activities of administrators could result in unauthorized activity at a database or server level. In addition, since unusual activities and their associated trends are not monitored, there is a risk of improper activity remaining undetected, thereby hampering the integrity of the system. There is an even greater risk if an intruder has compromised the system, manipulated the data and deleted all traces of the intrusion.

Recommendation # 12:

It is recommended that active monitoring of administrators' access to the PAXIS server and database be performed on a regular basis to ensure adequate controls over their use of the PAXIS application.

CBSA Response:

The CBSA audit trail strategy is currently under development and the framework will be completed by December 2006 in order to ensure required audit trails and log sharing activities are part of our Software Development Lifecycle (SDLC) for projects and systems. The CBSA will also review the current procedures and processes for monitoring administrators' access to the PAXIS server and database and implement appropriate control measures.

NATIONAL RISK ASSESSMENT CENTRE

Program description

3.113 In January 2004, the Government of Canada established the National Risk Assessment Centre (NRAC) within the Enforcement Branch of the CBSA. The Centre operates a number of initiatives and programs that relate to travellers. These include the Shared Lookout and High-Risk Traveller Identification (HRTI) initiatives with the United States. The Border Watch Line is also operated by the Centre.

3.114 The creation of the NRAC and the above initiatives were in response to the events of September 11, 2001 and recommendations outlined in the Customs Plan of April 2000, which promoted more reliance on intelligence and risk-based assessments to guide customs enforcement actions.

3.115 As reported above, the NRAC is responsible for operating the Border Watch Line (1-800 Tip Call Centre). Using a toll-free telephone number, members of the public may report information about cross-border criminal or suspicious activity. Such calls are directed to the appropriate CBSA regional operational unit for appropriate action. Although the caller's identity remains confidential, the information provided may be shared with domestic agencies and foreign customs organizations on a need-to-know basis, after the reliability of the information has been assessed by the CBSA.

3.116 A number of Standard Operating Procedures (SOPs) govern the day-to-day operations of the NRAC. In terms of information sharing activities, all disclosures, both within the CBSA and to external organizations, are subject to the restrictions contained in section 107 of the *Customs Act,* CBSA policy, and the Canada-United States MOU for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information.

The shared lookout initiative

Background

3.117 A lookout is an electronic file record created in the Integrated Customs Enforcement System (ICES) for specific travellers or vehicles based on risk indicators and other available intelligence. Canada and the United States have been sharing selected lookouts for a number of years. The automated or electronic sharing of lookout data began on February 6, 2004. Commercial (business) and postal lookouts are not shared under this initiative.

3.118 There are three categories of lookouts. The CBSA considers the categories protected information. Generally, they relate to threats to national security, or to the economic or social welfare of Canada.

3.119 The Canada-United States MOU for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information, signed on March 9, 2005, establishes the framework for the automated exchange of lookout information. A summary of the terms and conditions contained in the MOU is provided below:

- parties must acknowledge receipt of a lookout;
- parties must inform the other whether the lookout was accepted or rejected;
- if a lookout is rejected, the reasons must be communicated;

- the receiving country must comply with sending country's rules concerning the expiry, cancellation and archiving of the lookout;
- a third party lookout cannot be shared unless the sending country receives prior authorization from the third party;
- lookouts will not be shared with, or be made accessible to, unauthorized individuals;
- shared lookouts will be identified by a header;
- the receiving country may not arbitrarily cancel, modify or change the dates of a lookout; and
- the results of examinations undertaken as a result of a lookout must be shared with the country that issued the lookout.

3.120 As noted above, lookout information is stored in the CBSA's Integrated Customs Enforcement System.

Personal information

3.121 Lookout data identifies the subject according to available information. In addition to the subject's name, date of birth and gender, a lookout may contain a physical description of the individual and other specific identifying data.

3.122 A lookout also contains a narrative section that provides the rationale for the lookout and includes information that may increase its effectiveness.

3.123 Several types of lookouts may be shared under the Canada-U.S. agreement. These include lookouts related to national security threats and cross-border criminal activity.

Trans-border flow of personal information

3.124 The data flow begins with the entry of a lookout by the CBSA (normally a regional intelligence officer) or the U.S. Customs and Border Protection Agency (CBP). A lookout entered by the CBSA is chosen for sharing by the lookout authorizer (e.g., RIO) who is asked if he or she wants to share the lookout with the U.S. CBP. The lookout authorizer is also asked whether the lookout information is from a third party source (e.g., police agency) and, if so, whether they have obtained permission to share it.

3.125 The NRAC is responsible for reviewing CBSA shared lookouts prior to transmission to the U.S. As noted later (paragraph 3.132), not all shared lookouts are reviewed by the NRAC before they are communicated to the U.S.

3.126 Lookouts received from the U.S. are reviewed by NRAC staff to ensure that they meet established sharing criteria and contain sufficient information to enable a customs inspector to correctly action and respond upon interception.

3.127 According to information obtained from NRAC officials, the CBSA accepted a bulk transfer of approximately 17,500 records (existing lookouts) related to national security from the U.S. CBP in March 2003. These records were placed in the Canadian lookout system based on their active status and category type. The lookouts were loaded without prior screening. Subsequent to completing a review, 5,000 of the lookouts were removed from the CBSA system, leaving approximately 12,500 lookouts. This transfer of records was not part of the shared lookout initiative.

3.128 After the automated shared lookout initiative was implemented in February 2004, a second bulk transfer was completed to improve and update the information from the U.S. CBP in the Canadian lookout system. This second transfer was based on specific requirements and replaced the previous lookout records received. We were told that 4,000 met the requirements. These were individually vetted by NRAC personnel for, among other things, quality and practical use. As a result of this exercise, approximately 100 lookouts were removed from the Canadian system. NRAC officials further advised that the expiry dates for the remaining lookouts (approximately 3,900) were set at no more than one year from the date of transfer, with the option of extension as deemed necessary. We were also informed that less than ten of these lookouts remain active today.

3.129 In terms of the lookouts that were either not accepted for transfer or were subsequently rejected or cancelled as noted above, NRAC officials explained that this was due to the lack of sufficient detail to identify the subject(s), quality, usefulness or relevancy of the lookout. A number of duplicate lookouts were also rejected.

3.130 Resultant rates are one means of measuring the effectiveness of the lookout program. The CBSA defines "resultants" as enforcement actions that occur after a traveller has been flagged in a lookout and intercepted. Examples of enforcement actions include arrest, seizures of contraband, and the detection of smuggled goods. A lookout may also be created for the sole purpose of monitoring an individual's travel patterns and travel companions. While intelligence related interceptions may not result in an enforcement action, they are nevertheless effective from an intelligence gathering perspective. Further, resultant rates do not take the deterrence factor of lookouts into account. For example, an individual may avoid travelling across the border or refrain from carrying out certain activities.

Not all lookouts are subject to a vetting or review process before the CBSA shares them with the United States.

3.131 The audit found that a number of regional and headquarters intelligence officials are authorized to share lookouts locally with U.S. authorities when emergency circumstances exist – e.g., an imminent risk to national security, health or safety. Such lookouts are issued by telephone to a U.S. customs official. The audit found that not all locally issued shared lookouts are in response to an emergency or imminent risk.

3.132 One of the NRAC's roles is to review Canadian lookouts before they are transmitted to the United States. The objective of the review is to ensure that lookouts meet established criteria for sharing, contain sufficient information to be effective and do not contain information the disclosure of which is prohibited under law. Although not appearing as a systemic issue, a number of regional intelligence officers indicated that they have or would contact their U.S. counterparts directly to issue a lookout rather than having the lookout processed electronically through the NRAC. Given that lookouts can be shared on a real-time basis through the automated exchange, it is puzzling that the NRAC review process would be circumvented when emergency circumstances do not exist. In addition to providing a mechanism for reviewing the quality of data, the NRAC's involvement in the process ensures that all shared lookouts are captured for monitoring and auditing purposes.

Recommendation # 13:

It is recommended that the CBSA institute measures to ensure that all lookouts shared with the United States are transmitted through the National Risk Assessment Centre for quality control, monitoring and auditing purposes.

CBSA Response:

The CBSA will undertake a review of the existing processes for lookout sharing. It should be noted however that the NRAC and NTC exchange is limited to higher risk lookout categories only. Non NRAC and NTC exchanges to be addressed in Action Plan regarding Recommendation #2.

The personal identifying information on some lookouts is limited to an individual's name, which creates a risk that the wrong person could be subject to unnecessary secondary referrals at border crossings.

3.133 Attaching a date of birth to the name of a person for identification purposes is not a mandatory data element under the Canada-U.S. shared lookout initiative. This fact could increase the number of travellers who are referred to secondary examination on the basis of name only. Arguably "name-only" lookouts could increase the number of "no matches" or false positives – an individual who, upon secondary examination, is found not to be the person identified in the lookout. A study and analysis of the methodology used to positively identify individuals for lookout sharing has not yet been carried out. Therefore, there remains the risk that individuals may be deemed a high or unknown risk based on minimal data – name only.

3.134 As part of our examination, we randomly selected 125 lookouts for review. The sample was extracted from various types of lookouts – e.g., currency, narcotics, hate propaganda, liquor, kidnapping, missing children, general smuggling, terrorism. They included both CBSA-issued lookouts, and shared lookouts created by the CBSA on behalf of other Canadian law enforcement agencies. Approximately 20% of the sample were lookouts that had been issued by the U.S. and transmitted to Canada under the shared lookout initiative.

3.135 The 125 lookouts sampled, comprising 309 subjects (individuals), satisfied the established criteria for sharing under the Canada-U.S. automated lookout program. However, we found one Canadian-issued lookout where the identifying information was limited to the subject's name. We made the same observation in a number of cases where multiple subjects were listed on the lookout. In summary, there were 16 other lookouts that identified 27 individuals as subjects of interest. Of these, the identifying information for 10 of the individuals was limited to their name; there was no additional identifying information such as the person's address, driver's licence number or date of birth. These ten individuals were associated to other subjects, vehicles, addresses and other sources of information that would link them to the lookout. Nevertheless, there remains the potential that a referral to secondary may be based on name only.

A review of the effectiveness of the Canada-U.S. shared lookout initiative has not yet been undertaken.

3.136 The statistical data that the CBSA provided to the audit team would appear to suggest that the lookout resultant rate (see paragraph 3.130 above) in Canada is low. It is not clear whether this is an acceptable or useful rate given the nature and attributes of high-risk travellers. Moreover, the statistics relating to cancelled lookouts cannot distinguish between the lookouts that were cancelled because they were no longer valid and those that were cancelled because they resulted in false positives.

3.137 Any system used to identify high-risk travellers on the basis of intuition, physical indicators, intelligence or risk scoring – or a combination of one or more of the above – may result in some individuals being referred to secondary screening who are found to be of low or no risk. We believe it is in the interest of both the CBSA and the travelling public that such occurrences are kept to a minimum.

3.138 A comprehensive review of the effectiveness of the Canada-U.S. shared lookout initiative has not yet been undertaken. Therefore, it is not known whether the initiative produces better results than did previous methods of lookout sharing.

Recommendation # 14:

It is recommended that the CBSA evaluate the shared lookout system to determine both its effectiveness in identifying high-risk travellers entering Canada, and the extent to which it increases enforcement and intelligence resultants, while minimizing unnecessary referrals of travellers to secondary screening.

CBSA Response:

An evaluation of targeting in the CBSA will be initiated in 2006, and among other issues the use of lookouts will be an element of the targeting evaluation.

High-Risk Traveller Identification (HRTI) Initiative

Program description

3.139 Under the Canada-U.S. Smart Border Declaration and 30-Point Action Plan, Canada and the U.S. have committed to using technology and information sharing to more effectively identify high-risk travellers.

3.140 At the time of the audit, the HRTI initiative provided for the sharing of API as well as lookout, enforcement and passage history on a person between the CBSA and its U.S. counterpart, the U.S. CBP. More specifically, the HRTI tool facilitates the sharing of API data from the CBSA's Passenger Information System (PAXIS) and the U.S. Automated Targeting System-Passenger (ATS-P) system over a secure IT link. We were informed that the sharing of PNR data under the HRTI initiative will not begin prior to June 2006.

3.141 The CBSA's PAXIS has two components – a front-end data acquisition component, and a back-end analysis component. The front-end acquisition component involves the collection of API and PNR about airline passengers and crew from a carrier's Departure Control and Reservation system. When the API data elements are received, the system automatically retrieves the required PNR data for every individual on the flight.

3.142 The back-end analysis component involves running risk patterns, jointly established by the CBSA and the U.S. CBP, based on known indicators, trends and analysis, against a traveller's API/PNR in order to establish a risk score for the traveller. The risk patterns are comprised of various PNR elements, however the scores and risk levels attributed to them vary in accordance to the pattern they are assigned to. The risk score total is used to assess whether a traveller meets an established risk threshold of a particular risk pattern, which would theoretically identify the traveller as an individual who may require closer scrutiny or who is of high or unknown risk.

3.143 Once a particular risk pattern has been created, modifications can be made to any component of the risk pattern based on the analysis of results from the use of this data at the border. Both enforcement and intelligence information can trigger a modification.

3.144 The management of data exchanged under the Canada-U.S. HRTI initiative is established under the MOU for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information, signed in March 2005. A number of elements of the MOU support privacy and security, including the following:

- information is not to be provided in such a way as to allow one participant to have direct access to the information system of the other;
- access to information is to be administered on a need-to-know basis;
- general responsibilities with respect to information security and safeguards, including the institution of audit and tracking mechanisms are articulated in the MOU; and
- any further dissemination of data received under the MOU is subject to the "third party rule", which requires authorization from the sending party prior to the dissemination by the receiving party.

Personal Information

3.145 The data elements of the Advance Passenger Information (API) and Personal Name Record (PNR) are used for risk scoring purposes under the HRTI initiative.

3.146 API data elements are: name, date of birth, gender, document type, document number, the country that issued the document, and the date and estimated time of arrival. PNR captures information relating to a person as contained in the airline carrier's reservation or departure control records. A list of all PNR data elements is found in the text book below paragraph 3.99 of this report.

Trans-border Flow of Personal Information

3.147 The flow of personal information under the HRTI initiative is described below.

- When API/PNR data is received from commercial air carriers en route to Canada, the data is automatically scored against established risk patterns developed jointly by the NRAC and the U.S. National Targeting Centre (NTC). The risk scoring sub-system resides within the Passenger Information System (PAXIS).

- When a traveller meets the prescribed threshold, the following data are automatically sent to the U.S. NTC to query against its databases:

  - the individual's first and last name;
  - gender and date of birth;
  - travel document type;
  - travel document number;
  - country in which travel document was issued;
  - flight date and estimated time of arrival;
  - the risk patterns identified; and
  - the individual's threshold score.

- The NRAC reviews all information regarding any traveller that meets a threshold, including the risk score calculation, API/PNR information, information retained on CBSA databases and any information received from the U.S. NTC.

- Based on the information collected, the NRAC determines whether the establishment of a lookout is warranted and takes appropriate action.

3.148 The process that the NRAC follows in processing an information request from the U.S. mirrors the above description. NRAC staff conduct a manual review of all information (enforcement, passage history and lookouts) before it is sent to the U.S. NTC for its consideration.

Data exchanges do not occur under the following scenarios:

- an API record corresponds with a traveller in the information request, but there is no associated PNR or Departure Control System (DCS) data; or
- a PNR or DCS record corresponds with a traveller in the information request, but there is no associated API record.

The HRTI initiative has not yet been assessed to determine its effectiveness in identifying high-risk travellers.

3.149 The *Privacy Act* requires that the collection of personal information should be limited to that information which is necessary for the organization to carry out its legislative mandate. Given the volume and sensitivity of the personal information being exchanged between Canada and the U.S. under the HRTI initiative, there is a requirement – indeed, in our view, an obligation – for the CBSA to assess whether the benefits derived from the initiative warrant the intrusion on the privacy of the millions of travellers from whom API/PNR data are collected.

3.150 At the time of our audit, the CBSA's Evaluation Directorate had not conducted a study of the HRTI initiative as the phase involving the risk assessment of PNR data had not yet been implemented. It is expected that full implementation will be completed by June 2006.

3.151 Until a comprehensive assessment is done, the effectiveness of the HRTI tool in increasing the rate of interdiction and positive results (e.g., preventing the entry of inadmissible persons and prohibited goods, and collecting useful intelligence) remains speculative. In addition, the efficacy of the data elements and the algorithm used to process the data have yet to be validated or reliability tested. Further, the number of false positives that have occurred from outputs generated by the HRTI tool is, to date, unknown.

3.152 Two studies produced by the CBSA concerning the use of API/PNR data in Passenger Targeting Units (PTUs) were examined during the audit. These studies raised concerns about the quality and quantity of PNR data the Agency has received from certain airlines. Our review of these reports and our interviews with officials in the PTUs visited during the audit produced anecdotal evidence that inaccurate and incomplete PNR data may skew the risk scoring process. While we were informed that an enforcement action would not be initiated solely on the basis of API/PNR data, the risk remains that incorrect PNR data could result in a traveller meeting the established risk threshold. While a false negative (where a risk scoring tool fails to identify a high-risk individual) raises legitimate security concerns, false positives are of equal concern from a privacy perspective.

3.153 The undertaking of a comprehensive review of the automated risk assessment system to measure outcomes, including any unintended consequences to travellers, should help answer the question of whether the collection, use and disclosure of vast amounts of personal information can be justified from both security and privacy perspectives.

Recommendation # 15:

It is recommended that the CBSA undertake a review of the HRTI initiative as soon as practical, including an analysis of specific data elements used by the algorithm, to determine whether the system is:

- *generating an increase in interdiction rate or other positive resultants;*
- *resulting in an increase in the number of false positives; and*
- *producing results that justify collecting personal information on millions of travellers, as opposed to previous methods used to target high-risk individuals.*

CBSA Response:

The HRTI initiative has not yet been fully implemented. Full implementation is scheduled for June 2006 with an in-depth post-implementation evaluation planned for the following year. This review will explore all aspects of the HRTI including factors such as what data and analysis techniques generate positive results. Until this review can be undertaken, in response to the data quality issues identified in the post-implementation review of PAXIS, the CBSA has established a comprehensive data analysis function to monitor and analyze problems with the accuracy and completeness of passenger data that have a potential impact on the efficacy of the analysis and targeting activities.

The CBSA takes very seriously its responsibility for protecting the personal information of millions of travellers arriving in Canada. The CBSA goes to extraordinary means to ensure that the privacy of passenger data is protected by increasingly de-personalizing the information so that travellers' names are not visible to CBSA officials while they are carrying out analysis for the purpose of identifying trends and patterns which might help to improve the rate of interdiction of high risk individuals.

PRIVACY MANAGEMENT FRAMEWORK

Background

3.154 The concept and design of a privacy management framework for government departments and agencies are relatively new. Generally, organizations have yet to develop a comprehensive and cohesive framework for managing the personal information that they hold. To contribute to addressing this gap, the Privacy Commissioner recently recommended that the Treasury Board Secretariat (TBS) develop a model framework to guide privacy management in the federal public sector (page 31 of the Privacy Commissioner's 2004-2005 Annual Report to Parliament on the *Privacy Act* refers).

3.155 Generally, a Privacy Management Framework should:

- effectively communicate the importance of managing personal information to the organization and foster a commitment to building privacy into program management activities;

- establish clear objectives and standards for the collection, accuracy, security, use, disclosure, transmission, access, retention and disposal of personal information;

- clarify an organization's structures, roles and responsibilities relating to privacy, and provide a basis for determining the resources and skills needed for achieving sound privacy management practices;

- rely on sound risk management approaches, particularly through privacy impact assessments and threat and risk assessments;

- incorporate best practices and effective controls to promote compliance – integrating the best available privacy-enhancing technologies, and mechanisms for resolving disputes effectively and for identifying and correcting system weakness or privacy incidents; and

- promote accountability and continuous improvement of personal information handling practices through: program reporting, audit and evaluation, continuous monitoring of personal information handling practices, and the provision of ongoing privacy training to employees.

3.156 The scope of our examination was not designed to either assess the entire spectrum of the CBSA's security programs and activities, or identify specific cases of improper use or loss of personal information. However, privacy considerations are closely linked to security and the protection of personal information and can be affected by security generally. Therefore, we did examine the Agency's security related policies and procedures, its process for reporting security incidents, and the extent to which privacy breaches are reported internally.

3.157 Through interviews and examining documents we found evidence that the CBSA generally understands privacy and wishes to advance its privacy management practices. Matters related to privacy and personal information management are included in a variety of CBSA documents both in draft and final forms. Much of the documentation that we reviewed had been either recently created by the CBSA, or inherited from its legacy organization, the former Canada Customs and Revenue Agency. The documentation included:

- security policies and procedures – CCRA Finance & Administration Manual
    - identifying classified and protected information and assets
    - storage, transmittal and disposal of sensitive information and assets
    - protection of classified and protected information and assets outside the workplace
    - personnel security screening
    - access control
    - reporting of security incidents
    - access to Agency computer systems
    - IT security standards and practices
    - remote access to and from Agency computer systems
    - TRAs for IT systems
    - security reviews and inspections of computer systems
    - usage of personal computers at employee residences
    - logging and monitoring of employee access to client data
    - internal investigations into alleged or suspected employee misconduct
- policies governing the use and disclosure of customs information
- delegation orders for the administration of the CBSA's obligations under the *Access to Information Act* and *Privacy Act*
- regional training packages, including learner's guide, for disclosure of customs information under section 107 of the *Customs Act*
- privacy impact assessments and threat and risk assessments undertaken by the CBSA
- memoranda of understanding or written agreements regarding access to and use of information held under the control of the CBSA
- a new draft guide for developing written collaborative arrangements with provinces, territories and other federal departments and agencies.

3.158 The CBSA also relies upon Treasury Board directives, policies and instruction for ensuring compliance with the *Privacy Act*. There is also reliance on informal communication links as may be established by individuals out of immediate or local necessity. Finally, we were also informed that the CBSA intends to develop its own set of privacy and security policies and guidelines to replace and update those that were inherited from the CCRA. These will take into consideration the practices and needs of programs for which the CBSA is responsible.

The time is opportune for the CBSA to develop and implement a privacy management framework.

3.159 Despite the existence of the documentation noted above, and the fact that the Agency intends to develop privacy policies and guidelines, our audit found that the CBSA lacks a comprehensive and cohesive privacy management framework – one which is integrated closely with operations across the organization. Several important elements of a strong framework are either absent, incomplete or need to be updated.

3.160 A key feature of a privacy management framework is the ability to identify, investigate and report on privacy breaches involving any alleged inappropriate collection, use, disclosure or disposal of personal information. This is an area we examined and report in more detail. The information that we obtained during the audit did not allow us to clearly understand how the CBSA identifies and reports privacy breaches across the organization. The following captures what we learned and observed through interviews with security officials and through our review of files and policy documents in relation to identifying and reporting of privacy breaches.

- The President of the CBSA is briefed monthly on security incidents that are reported to CBSA Headquarters, as well as any cases involving the investigation of employee wrongdoing.

- The existing policies and procedures that were in use for security incident reporting and management at the time of our examination deal primarily with such defined things as:

    - theft, loss or destruction of revenue, money, seized, held or other assets;
    - abuse, threats, stalking and assaults against employees;
    - suspected or actual compromise of protected and/or classified information;
    - malicious codes and virus alerts/attacks on communication or IT systems;
    - destruction, mutilation, alteration, or falsification of records;
    - loss, theft or misuse of identification/access cards, building passes; and
    - incidents impacting physical security of a building or facility.

- The CBSA has 14 categories of security incidents. Nothing exists in CBSA policy, procedures and reporting forms specific to privacy that describes how the Agency would handle occurrences of improper collection, use or disclosure of personal information (accidental or otherwise) by CBSA employees.

- Since the CBSA was created in December 2003, 30 Security Incident Reports (SIRs) have been filed with the Security Section at CBSA Headquarters. We were unable to determine whether all incidents involving breaches in the handling of personal information were reported to Headquarters from the regions.

- Of the SIRs that we looked at:

    - Fifty percent of the security incidents did not involve personal information.

- Of the 50% of incidents that either exposed personal information or placed the information at risk:

    - four related to lost or stolen computers, mainly laptops (the reports indicate that these computers may have contained personal information, but that one had encryption protection);
    - two involved the loss of, or improper access to, customs inspector notebooks;
    - three concerned mail lost in transit;
    - three involved unauthorized physical access to restricted work areas;
    - two related to unauthorized IT access through one employee sharing a user account with a colleague; and
    - one incident related to a password breach.

- We noted some cases where the security incident reports raised questions about whether the computers may have contained sensitive customs or personal information, but the responses to these questions were not provided in the narrative of the report.

- We also noted from our interviews that the CBSA could not readily tell us either how many employees were engaged in flexible work arrangements (i.e., telework), or the number and type of computer devices that had been assigned to staff for use outside CBSA premises. External working environments involving customs and personal information, coupled with new technology (e.g., Blackberry) raise physical, IT, operational and privacy challenges. These personal digital assistants (PDAs) require unique safeguards to mitigate risks that may not be the same as those used in a standard work environment.

3.161 We also found that, at the time of our audit, the Agency had no formal internal policy defining when the Access to Information and Privacy Division (ATIP) of the CBSA would or should be advised of:

- any security breaches and internal wrongdoing investigations that involve personal information, or
- complaints received and addressed by CBSA's operational units (e.g., border crossing, airport, etc.) from individuals who allege that their privacy rights were violated.

The Agency informed us that such a process will be established and included in CBSA policies currently under development.

3.162 Further, the new materials for privacy training sessions that we examined did not define what would constitute a "privacy breach". Nor did the materials outline how privacy breaches (e.g., improper use, disclosure or loss of personal information) would be investigated and reported.

3.163 As a final note, there have been no audits of the CBSA's process for reporting security incidents. Accordingly, the CBSA is unable to attest to the completeness and accuracy of this process, and whether it captures all incidents affecting personal information, regardless of whether the incident was the result of deliberate wrongdoing, or considered accidental.

3.164 We believe the time is opportune for the CBSA to articulate and implement a privacy management framework. The objective would be to improve the systems and processes for observing and strengthening control over the collection, use, disclosure, retention and disposal of both personal information generally, and personal information that flows across the border to other countries.

3.165 In designing and implementing a privacy management framework for the CBSA, we suggest that the Agency consider:

- designating a Chief Privacy Officer (CPO) with a clear mandate and corporate role to promote privacy awareness and compliance with privacy legislation and established information management practices. While a senior official has been identified as CPO, this had not been made official through a formal delegation with a defined mandate at the time of our audit.

- creating a Committee of senior managers to oversee the development of a privacy management framework and to plan, monitor and coordinate actions taken to strengthen privacy practices, including the development of privacy policies. This Committee would also ensure that privacy impact assessments (PIAs) are completed when required, that requisite guidance and training are provided to program areas on privacy issues, and various agreements governing the exchange of personal information are current and followed throughout the CBSA.

- creating a departmental privacy policy that clearly assigns roles and responsibilities and identifies where privacy practices would be a key element in evaluating the performance of employees. The policy should also articulate expectations for managing and controlling trans-border flows of personal information throughout its life cycle. We note that a formal CBSA policy dedicated to privacy has not yet been issued.

- implementing regular performance monitoring through means such as automated identification and reporting of unusual IT transactions, analysis of system use patterns, and internal privacy audits. These audits would both help to ensure consistent practices, and provide assurance to senior management that personal information is being managed in compliance with the *Customs Act*, the *Privacy Act*, and applicable internal policies and information sharing agreements. Such mechanisms are not prominent or featured at this time.

- providing regular and ongoing training sessions on the administration of – and compliance with – the *Privacy Act*. The CBSA began providing training sessions on privacy during our audit. While no training was delivered during fiscal year 2004-2005, since that time sessions have been delivered in six regions. The CBSA intends to deliver privacy training courses at least once in each region prior to March 2006. With these efforts and the introduction of an ongoing training strategy and plan, the level of privacy awareness and compliance will undoubtedly increase.

- establishing a reliable and comprehensive system for capturing privacy complaints and incidents across the CBSA (regions, ports of entry included) to ensure they are reported and remedied.

3.166 Once a framework has been established, the CBSA can then prioritize the implementation of the various elements of the framework and use it as a point of reference in guiding future decisions and actions.

3.167 While we recommend that the Agency establish a privacy management framework, it should be noted that no evidence surfaced during the audit to indicate that the CBSA has mishandled personal information. At the same time, it must be recognized that since many cross-border exchanges with the United States are verbal, and since detailed records of the disclosures were lacking, there remains an open question as to whether the CBSA is managing personal information appropriately in all cases.

Recommendation # 16:

It is recommended that the CBSA develop a comprehensive privacy management framework tailored to its particular needs. It should use the framework for guiding improvements to privacy related policies, systems, procedures and practices. As part of this exercise, the CBSA should clarify and consolidate privacy incident reporting and seek ways of strengthening the monitoring of the collection, use and disclosure of personal information in daily operations.

CBSA Response:

We agree. The CBSA will work with the Treasury Board Secretariat (TBS) and the Office of the Privacy Commissioner to determine gaps in our Privacy Management Framework and we will welcome their advice.

PUBLIC REPORTING OF TRANS-BORDER DATA FLOWS

Background

3.168 As an extension of the review of the CBSA's activities in the area of trans-border data flows, we examined how and the extent to which the CBSA informs Parliament and the Canadian public of trans-border disclosures of personal information.

3.169 The study involved a review of the following:

- *Info Source*
    - Sources of Federal Government Information 2004-2005
- Official reporting documents:
    - Reports on Plans & Priorities
    - Departmental Performance Reports
    - Annual Reports to Parliament
    - Annual Reports on the administration of the *Access to Information Act and Privacy Act*
- Website documents

3.170 We examined the personal information banks listed and described in Info Source for references to information sharing with, or disclosures to, the United States or other foreign entities. Turning to the official reporting and Website documents, we used global computer searches to find references to information "sharing" or "exchange" in contexts where the involvement of U.S. or other foreign organizations is either stated or may reasonably be inferred.

The CBSA could improve the information in its vehicles for informing Canadians and Parliament about the trans-border release of personal information.

3.171 In essence, the public should be able to find adequate information in publicly available documents (either print or electronic) on what personal information the CBSA shares with other countries. However, while we found some exceptions among publicly available reports, references to the CBSA's activities relating to the flow of data across borders are brief. They contain little elaboration and do not clearly indicate the extent to which personal information is shared with other countries. In some instances, the Agency provides more information on its Website than in reports to Parliament or in Info Source (the publication that provides an account of the personal information held by the Agency and related programs). Our observations are summarized below:

3.172 Info Source

- Eleven of the CBSA's personal information bank descriptions referred to information or intelligence sharing with foreign organizations. Of these, only three provided significant details on these sharing activities.
- The specific foreign organizations with which information is shared were identified in only three personal information banks. References to foreign organizations were general and non-specific in other instances – e.g, "United States authorities, foreign law enforcement and investigative agencies."
- Authorities for releasing information to foreign governments were identified in only general terms in five instances as being "pursuant to an agreement or arrangement in order to conduct a lawful investigation or administer or enforce any law".
- There was no explicit reference to information sharing with the United States or other foreign governments in the Advance Passenger Information/Passenger Name Record (API/PNR), Passenger Information System (PAXIS) or the Integrated Customs Enforcement System (ICES) personal information bank descriptions.
- The Customs Intelligence Records personal information bank (CBSA PPU 015) has not been identified for inclusion in the next Info Source publication. This personal information bank retains information used by the CBSA as well as domestic and foreign law enforcement and investigative agencies.

3.173 Official Reporting Documents

(1) *2005-2006 Report on Plans and Priorities*

- This document referred to sharing of information and/or intelligence with foreign organizations under four rubrics. However, it contained little elaboration, and it did not clearly indicate the extent to which personal information is involved.

(2) Departmental Performance Report ending March 31, 2004

- The report mentioned the sharing of information and/or intelligence with foreign organizations under 11 rubrics. Again, there was insignificant elaboration and no clear indication of the extent to which personal information was involved. In five instances, information sharing was referenced in connection with the National Risk Assessment Centre (NRAC) and the Joint Passenger Analysis Units (JPAU). It should be noted that the Canada-U.S. co-located JPAUs are no longer operational. Information sharing is also referred to, in general terms, in connection with the Canada-U.S. Smart Border Declaration.

(3) *Annual Report to Parliament 2005-2006 Report on Plans and Priorities*

- At the time of the audit, the CBSA had not yet published an annual report to Parliament.

(4) *Access to Information and Privacy Annual Report*

- At the time of the audit, the CBSA had not yet published an annual report on its administration of the *Access to Information* and *Privacy Acts*.

3.174 CBSA Website

- Eight documents referred to the practice of sharing personal information with foreign governments. Only one – a fact sheet relating to API/PNR data and the PAXIS data bank – described the practice in significant detail. The other references were included on fact sheets that relate to the Smart Border Declaration, the National Risk Assessment Centre, the Free and Secure Trade (FAST) program, immigration intelligence, strengthening customs examinations at airports, and in-transit container targeting at seaports.
- With the possible exception of the fact sheet on API/PNR and the PAXIS data bank, none of the documents found on the CBSA's Website provided enough information about trans-border information sharing to yield a clear picture about what information is shared and when, and for what purposes.

Recommendation # 17:

It is recommended that the CBSA review its personal information holdings to ensure that all personal information banks are listed in the next publication of Info Source, as required pursuant to section 11 of the Privacy Act.

Recommendation # 18:

It is further recommended that the CBSA examine all descriptions of personal information banks to ensure that all uses of the information therein—including the trans-border sharing of information with foreign governments – are adequately reflected.

CBSA Responses to Recommendations # 17 and # 18:

The CBSA will continue to work with the Treasury Board Secretariat to ensure existing and proposed Personal Information Banks accurately reflect with whom, and why, we share information, including the work we perform with our international partners.

3.175 We also believe that the CBSA, in conjunction with the Treasury Board Secretariat and other government departments, should assess other strategies for better informing Parliament and the public about the sharing of personal information with other countries. This assessment should include ways to improve the information in existing annual reporting mechanisms. Another possible strategy might be a special government-wide report on this issue on a periodic basis (e.g., in conjunction with review of the *Anti-Terrorism Act*) or the collective use of the Info Source publication, annual reports and departmental websites to make personal information handling activities more transparent and understandable for Canadians and Parliament. Transparency supports public accountability and is one of the 10 fair information principles embodied in the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

3.176 Our examination of the reporting of four other entities yielded similar results. It confirmed that the CBSA is not the only organization that needs to provide better information on its activities in the area of trans-border data flows. Accordingly, we will also be pursuing the matter with the Treasury Board Secretariat.

Recommendation # 19:

It is recommended that the CBSA, in conjunction with the Treasury Board Secretariat, assess alternative strategies and means of better informing Parliament and the public about the sharing of personal information with other countries.

CBSA Response:

The CBSA notes that departmental reporting of trans-border data flows is an issue that the Office of the Privacy Commissioner intends to pursue with the Treasury Board Secretariat.

The CBSA will independently approach the Treasury Board Secretariat to discuss potential strategies that could be used by our Agency -- and perhaps other federal agencies -- to improve transparency surrounding the nature of key international relationships, while also respecting our international obligations concerning confidentiality. The CBSA will explore with the Treasury Board any suggestions the Office of the Privacy Commissioner may have in this regard.

APPENDIX A

LIST OF RECOMMENDATIONS

Customs Enforcement

1. ***It is recommended that the CBSA, as part of strengthening its privacy management framework, seek to update and strengthen its personal information sharing agreements with the United States, including the establishment of processes that provide mutual assurance that trans-bordered personal information is accorded appropriate protections.***

2. ***It is recommended that the CBSA formulate an action plan to address verbal exchanges of personal information. Such a plan should consider:***

    - ***determining the extent to which customs information is being shared verbally with United States customs authorities and implement measures to ensure that all disclosures consistently comply with governing agreements and policies;***

    - ***implementing measures to ensure that all disclosures of personal information are recorded as required under CBSA policy;***

    - ***issuing a communiqué to all staff regarding the approval process governing disclosures under subsection 107(8) of the Customs Act, and reinforce the policy requirements by including a specific module in the delivery of Section 107 and Privacy Act training sessions; and***

    - ***monitoring compliance with policies governing cross-border exchanges of data to ensure that adequate management controls are in place to protect personal information from unauthorized disclosure.***

3. ***It is recommended that the CBSA implement ways and means of capturing all trans-border data exchanges for program management and accountability purposes. This might include – but is not limited to – the construction of data-flow diagrams, modifications to existing information systems to reliably record and identify all sharing activities with foreign governments.***

Integrated Customs Enforcement System (ICES)

4. ***It is recommended that the CBSA work with its U.S. counterparts to provide mutual levels of assurance that respective IT security controls are adequate to protect the privacy of citizen data in shared lookouts. In this regard, specific consideration could be given to extending Service Level Agreements to include descriptions of the processes to delete shared data upon expiry or cancellation, and the requirement for regular privacy and security audits.***

5. ***It is recommended that the CBSA modify the ICES application to ensure that the logging capacity includes when an ICES printout is made.***

6. ***It is recommended that the CBSA establish and communicate the roles and responsibilities of all designated IT officials in the organization, including updating job descriptions and organizational charts.***

7. ***It is recommended that the CBSA continue its efforts to create a cohesive security management framework. It should audit this framework within a year of its implementation to ensure that it is operating efficiently to protect customs and personal information. We also request that the CBSA provide the results of this audit to the Office of the Privacy Commissioner of Canada.***

8. ***It is recommended that CBSA log and monitor database administrators' access to and the operations performed on the ICES database.***

Passenger Information System (PAXIS)

9. ***It is recommended that a formal service level agreement be implemented between the U.S. and Canada to include mutually agreed security standards (based on the Government of Canada MITS security standard and standards on data quality and screening) so that each party takes steps to ensure that shared personal information is complete, current and accurate.***

10. ***It is recommended that a standard system rights checklist be used when a change in an employee's roles, responsibilities or employment status requires his or her manager to evaluate what system access rights the employee needs, what new system access permissions are required, and what permissions should be revoked.***

11. ***It is recommended that the PAXIS Support Desk Document be updated to include guidelines for revoking system access rights. We also recommend that CBSA Human Resources refer to the checklist to ensure that employees who change positions, those on long-term leave and individuals who have left the organization have had their system access rights reviewed and revised or deleted accordingly.***

12. ***It is recommended that active monitoring of administrators' access to the PAXIS server and database be performed on a regular basis to ensure adequate controls over their use of the PAXIS application.***

National Risk Assessment Centre (NRAC)

13. ***It is recommended that the CBSA institute measures to ensure that all lookouts shared with the United States are transmitted through the National Risk Assessment Centre for quality control, monitoring and auditing purposes.***

14. ***It is recommended that the CBSA evaluate the shared lookout system to determine both its effectiveness in identifying high-risk travellers entering Canada, and the extent to which it increases enforcement and intelligence resultants, while minimizing unnecessary referrals of travellers to secondary screening.***

15. ***It is recommended that the CBSA undertake a review of the HRTI initiative as soon as practical, including an analysis of specific data elements used by the algorithm, to determine whether the system is:***
    - ***generating an increase in interdiction rate or other positive resultants;***
    - ***resulting in an increase in the number of false positives; and***
    - ***producing results that justify collecting personal information on millions of travellers, as opposed to previous methods used to target high-risk individuals.***

Privacy Management Framework

16. ***It is recommended that the CBSA develop a comprehensive privacy management framework tailored to its particular needs. It should use the framework for guiding improvements to privacy related policies, systems, procedures and practices. As part of this exercise, the CBSA should clarify and consolidate privacy incident reporting and seek ways of strengthening the monitoring of the collection, use and disclosure of personal information in daily operations.***

Public Reporting of Cross-Border Data Flows

17. ***It is recommended that the CBSA review its personal information holdings to ensure that all personal information banks are listed in the next publication of Info Source, as required pursuant to section 11 of the Privacy Act.***

18. ***It is further recommended that the CBSA examine all descriptions of personal information banks to ensure that all uses of the information therein—including the trans-border sharing of information with foreign governments – are adequately reflected.***

19. ***It is recommended that the CBSA, in conjunction with the Treasury Board Secretariat, assess alternative strategies and means of better informing Parliament and the public about the sharing of personal information with other countries.***

APPENDIX B

AUDIT EVALUATION CRITERIA

The evaluation criteria for this audit are principally derived from obligations set out in sections 4 to 8 of the *Privacy Act*, the Government Security Policy, Treasury Board policies, guidelines and related documents governing the management of personal information.

In addition, some best practices criteria have also been adapted from Schedule 1 of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA)*.

Accountability (Principle 1 *PIPEDA*):

Criteria:

The organization must designate individual(s) who will oversee and coordinate the organization's activities to ensure the accountability for the organization's compliance with all privacy obligations.

Those individuals may delegate specific roles and responsibilities across the organization for ensuring privacy and security protections of its personal information holdings.

The organization shall use contractual or other means to ensure that third parties provide a comparable level of privacy protection as does the originating organization.

Note: Reference is made to criteria for information sharing agreements and contracting out. For information held by a government institution the standard would have to be as good as or better than that provided by the *Privacy Act*, Government Security Policies and TB Guidelines.

Organizations shall implement policies and practices to give effect to the principles, including implementing procedures to protect personal information; establishing procedures to receive and respond to complaints and inquiries; training staff and communicating to staff information about the organization's policies and practices; and developing information to explain the organization's policies and procedures.

Openness (Principle 8 *PIPEDA*)

Criteria:

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

The information made available shall include the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded; the means of gaining access to personal information held by the organization; a description of the type of personal information held by the organization, including a general account of its use; a copy of any brochures or other information that explain the organization's policies, standards, or codes; and what personal information is made available to related organizations (e.g., subsidiaries).

Note: An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its activities and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to individuals, provide online access, or establish a toll-free telephone number.

Identifying Purposes (Principle 2 *PIPEDA*):

Criteria:

The organization shall document the purposes for which personal information is collected.

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected.

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose.

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

Note: There may be exceptions to this principle, where the collection is done according to law and information provided to the individual may result in less or inaccurate personal information being collected.

Collection of personal information (Sections 4 and 5 of the *Privacy Act):*

Criteria:

Government institutions shall collect personal information only when it relates directly to an unauthorized program or activity of the institution.

Subject to exceptions referred to in subsection 5(3) of the *Privacy Act*, government institutions are required to inform individuals of the purpose for which the information is being collected and the intended uses to be made of it.

Wherever possible, government institutions shall collect personal information – intended to be used for an administrative purpose – directly from the individual to whom it relates.

Consent (Principle 3 *PIPEDA*)

Criteria:

Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

Limiting Collection (Principle 4 *PIPEDA*)

Criteria:

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified.

Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the openness principle. (Principle 8 of PIPEDA also refers).

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

Use of personal information (Subsection 6(2), section 7 and subsection 9(4) of the *Privacy Act)*

Criteria:

Government institutions shall take all reasonable steps to ensure that personal information that is used for an administrative purpose is as accurate, up-to-date and complete as possible. (Accuracy – Principle 6 of PIPEDA also refers).

Without the consent of the individual to whom it relates, personal information shall only be used by a government institution for the purpose for which it was collected, or for a use consistent with the original purpose, or for a purpose for which the information may be disclosed within or outside the institution under subsection 8(2) of the *Privacy Act*.

When personal information is put to a consistent use that is not listed in the personal information bank description in *Info Source*, such a use must be reported to the Privacy Commissioner and included in the next statement of consistent uses set out in *Info Source*.

(See also Limiting use, disclosure and retention – Principle 5 PIPEDA)

Use – Data Matching (Treasury Board Policy on Data Matching)

Criteria:

Government institutions must ensure that their data matching programs are designed and conducted in accordance with the principles of fair information practices embodied in the *Privacy Act* and in compliance with the Treasury Board Policy on Data Matching.

Limiting use, disclosure and retention (Principle 5 *PIPEDA*)

Criteria:

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods.

Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made.

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous.

Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

Accuracy (Principle 6 *PIPEDA*)

Criteria:

Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.

An organization shall not routinely update personal information, unless such a process is necessary to fulfill the purpose(s) for which the information was collected.

Disclosure of Personal Information (Section 8 of the *Privacy Act*)

Criteria:

Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed to a third party except in the limited number of circumstances established in subsection 8(2) of the *Privacy Act*.

Paragraph 8(2)(f) of the *Privacy Act* permits a federal government institution to disclose personal information to the government of a foreign state, an international organization of states or an international organization established by the government of states – or any institution of any such government – for the purpose of administering any law or carrying out a lawful investigation.

Such disclosures should be governed by a written collaborative agreement between the parties with appropriate data protection provisions contained therein.

Disclosure – Personal Information Sharing Agreements (Criteria developed from a variety of sources)

Criteria & Considerations:

1. Parties to Agreement
Does the agreement: a) clearly identify the public bodies, levels of government or other organizations involved in this sharing or exchange of personal information? b) name any third party contractors or service providers who will have access to personal information?
2. Authority
Does the agreement: a) define the legal authority – law, agreement or treaty permitting the parties to enter into an agreement for the sharing or exchange of personal information? b) define the legal authority governing the respective program/activities of the parties relevant to the agreement?

3. Purpose of agreement

Does the agreement:

a) identify the general intent of the information exchange?
b) identify if there will be a one-way or reciprocal sharing of personal information?
c) identify for each of the purposes or reasons stated in the agreement, the data elements or a description of the personal information to be shared or exchanged?
d) differentiate between the data elements exchanged in a reciprocal arrangement -- are the parties using different data elements?
e) indicate whether common client identifiers are used and, if so, what are they?
f) identify the sources of the personal information?

4. Accountability

Does the agreement:

a) specify the responsibilities of each party for carrying out the terms and conditions of the agreement as well as designate who within each party is accountable?
b) specify who has legal control of the shared personal information?
c) indicate whether or not the parties have common practices and procedures for complying with various elements of the agreement?
d) explain that each party will be responsible for responding to requests for access to, and the correction of, personal information under their control?
e) specify that each party will be responsible for the actions of its employees, agents or contractors with respect to the use, disclosure and disposition of the personal information that is subject to the agreement and applicable privacy laws?
f) specify whether the shared personal information is subject to any other access or privacy laws, regulations or guidelines beyond the laws of the disclosing party? Note: U.S. privacy laws generally apply to U.S. citizens and permanent residents only.

5. Mechanism for the sharing/exchange of personal information

Does the agreement describe the:

a) methods or procedures that will be used to share the personal information?
b) level of access rights to personal information of the respective parties, based on the need-to-know principle?

6. Obtaining consent from or notification to any affected parties

Does the agreement include a provision:

a) establishing how (or if) data subjects are aware of the sharing activity?
b) that provides reference to exceptions to the consent rule?

7. Use of personal information

Does the agreement:

a) clearly identify what uses are to be made of personal information shared under the agreement?
b) contain limitations or prohibitions against secondary uses of the information for purposes other than those listed in the agreement?

8. Disclosure to third parties (including contractors and subcontractors)

Does the agreement:

a) list the third parties to which personal information may be disclosed or provide categories of third parties?
b) clearly define the purposes and circumstances under which personal information can be disclosed to third parties as well as the procedures that must be followed to effect such disclosures?
c) permit disclosure for purposes other than those specified in the agreement (e.g., research and statistical purposes or program planning, forecasting or evaluation purposes)?
d) state that the terms of the agreement apply to any third party disclosure, including a requirement that third parties comply with the fair information principles to safeguard personal information?

9. Accuracy

Does the agreement:

a) identify the steps that will be taken to ensure that personal information is accurate, complete and up-to-date?
b) contain a clause that deals with the handling of requests for correction?
c) state that the substance of a request for correction should be communicated to those parties in receipt of disclosed information?
d) contain a clause stating that the parties must verify the personal information with the originating agency before it is used to make an administrative decision about an individual?

10. Security

Does the agreement include:

a) key administrative, personnel, technical, IT and physical safeguards and controls that are required to protect the security of the personal information shared (e.g., measures to secure the transmission of personal information and measures to prevent unauthorized access, use or disclosure)?
b) does the information sharing agreement establish the requirement for a Threat and Risk Assessment (TRA), including an assessment of the risks to the personal information that may be engendered by the arrangement?

11. Retention and Disposal

Does the agreement:

a) specify how long the shared personal information is to be kept and whether the information is to be returned to the source or securely destroyed by the recipient(s)?
b) indicate what will happen to the personal information exchanged upon the termination of the agreement?

12. Data Matching and Data Linkage

Does the agreement include any data matching, linkage or profiling activities carried out by either party further to the sharing of personal information?
(Note: *see Treasury Board Policy on Data Matching*)

13. Privacy Impact Assessment

Does the information sharing agreement define a new or different kind of arrangement for the sharing of personal information that would require the completion of a Privacy Impact Assessment under Treasury Board Policy?

14. Unauthorized Use or Disclosure

Does the agreement:

a) establish notification procedures in the event of discovery of an unauthorized use or disclosure of the shared personal information?
b) state that the party in breach should promptly notify the other party?
c) specify the consequences of using or disclosing the personal information without authority?

15. Disputes

Does the agreement outline a process to be followed to resolve any disputes relating to the terms of the agreement?

16. Audits

Does the agreement:

a) include a clause allowing for periodic audits of the sharing arrangements to ensure compliance with the terms of the agreement?
b) require that results of such audits be shared with the other party?
c) reference audit trail tools and methods to be used to track access to records, modification of records and disclosures?
d) reference the Privacy Commissioner's right to access information held by federal government institutions for the purpose of conducting investigations and audits under the *Privacy Act*? Note: there may be other bodies with similar statutory powers.

17. Amendments/Renewal and Cancellation

Does the agreement provide for:

a) amendment(s) and renewals in writing with the mutual agreement of the parties?
b) cancellation by one or the other parties?

18. Changes that affect the Agreement

Does the agreement include:

a) an undertaking that the parties will provide written notification of any legislative, regulatory or policy changes that affect the agreement.

19. Time frame
Does the agreement set out a time frame for its: a) existence? b) review by the parties?
20. Definitions
Does the agreement include definitions of any terms that may be unique to the agreement?
21. Signing authority and contact names
Does the agreement: a) have explicit sign-off by the "heads" of the public bodies (or by those officials with delegated authority to sign such agreements) and by officials at similar levels in other organizations? b) contain: contact names, titles, addresses and phone numbers of appropriate officials of all parties charged with administering various aspects of the agreement?

Disclosure -- Contracting out (Criteria developed by the OPC)

Criteria:

Personal information which is collected, used, processed, disclosed, held or disposed of on behalf of a government institution, or in fulfillment of a contract with a government institution, shall be managed in conformity with the principles of fair information practices embodied in the *Privacy Act* and the *Privacy Regulations.*

When a private sector agency or contractor manages personal information on behalf of a government institution, the contract must specify that such personal information is deemed to be under the control of the government institution and is subject to the *Privacy Act.*

The contract must also stipulate, where applicable, how the service provider or contractor will meet the Act's requirements in terms of managing the personal information it will handle while carrying out the contract.

The contract should also recognize the Privacy Commissioner's right of access to the personal information for the purposes of conducting audits and investigations.

(For additional criteria, refer to above checklist for Personal Information Sharing Agreements)

Safeguarding Personal Information (Sections 6, 7 and 8 of the *Privacy* Act)

Criteria:

Government institutions must have in place appropriate security measures to ensure that, throughout its life cycle, personal information under their control is protected and not vulnerable to unauthorized access, use, disclosure, alteration or destruction.

E-mail & Facsimiles:

> There are many reasons why sending personal information by e-mail or fax poses security risks. If not sent or received by secure means, the information may be intercepted or exploited, or received in error by someone who is not authorized to receive the information. Identifiable personal information should not be sent by e-mail or fax, unless by secure means (.e.g., encrypted message, secure fax in a secure area).

Government institutions must, therefore, adopt security measures that protect the confidential nature of personal information being transmitted electronically.

Safeguards (Principle 7 *PIPEDA*)

Criteria:

The security safeguards must be adequate to protect personal information against loss or theft, as well as unauthorized access, disclosure, use, modification or reproduction.

Organizations shall protect personal information regardless of the format in which it is held.

Note: The nature of the safeguards will vary depending on the sensitivity and amount of personal information collected, its distribution, the format of the data and the method of storage.

The methods of protection should include adequate: physical measures (e.g., locked filing cabinets and restricted access to offices); organizational measures (e.g., security clearances and limiting access on a need-to-know basis); and technological safeguards (e.g., the use of passwords and encryption to protect personal information).

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

Care shall be exercised in the disposal or destruction of personal information to prevent unauthorized access to it.

Retention and Disposal (Subsection 6(1) of the *Privacy Act* and paragraphs 4(1) and (2) of the *Privacy Act*)

Criteria:

Personal information must be retained and disposed of in accordance with approved records retention and disposal schedules.

Except as otherwise provided in law or where the individual consents to earlier disposal, personal information that has been for an administrative purpose – that is, in the decision-making process that directly affects the individual – must be kept for a minimum of two years after the last time it was so used.

Records should be properly disposed of in a manner consistent with their security classification.

Access (Principle 9 *PIPEDA*)

Criteria:

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information.

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

In providing an account of third parties to which it has disclosed personal information, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

Where personal information has been transferred to a third party contractor, the organization must ensure that it obtains copies of records relevant to the access request from the third party.

Where personal information has been disclosed under an information sharing agreement, the organization must ensure that it keeps the originals for any access requests for these records.

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. The amendment may involve the correction or deletion of information, or the inclusion of additional information. Where appropriate, the amended information shall be transmitted to third parties having access to the information at issue.

Challenging Compliance **(Principle 10 *PIPEDA*)**

Criteria:

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant redress procedures (including the right of complaint to the Office of the Privacy Commissioner of Canada).

An organization shall investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.

OTHER AUDIT CRITERIA

Awareness of the *Privacy Act*

Compliance with the spirit and specific requirements of sections 4 to 8 of the *Privacy Act* depends largely on the degree of understanding of the Act’s provisions by the persons responsible for administering the Act for the institution and, to a lesser degree, by other employees of the institution.

Criteria:

Government employees handling personal information must be aware of their obligations under the *Privacy Act,* including restrictions on disclosures of personal information.

The government institution must provide employees with appropriate *Privacy Act* training and documentation to ensure that they are kept up-to-date on their privacy obligations.

InfoSource (Sections 9, 10 and 11 of the *Privacy Act*)

Criteria**:**

As a complement to sections 4 to 8 of the *Privacy Act*, sections 9, 10 and 11 of the Act require that all personal information holdings must be described and published in *Info Source* as Personal Information Banks or as classes of personal information.

Government institutions must ensure that all such descriptions are as complete, up-to-date and accurate as possible.

APPENDIX C

LIST OF ACRONYMS	
ACRONYM	**NAME**
API	Advance Passenger Information
ARS	Airline Reservation System
CBSA	Canada Border Services Agency
CBP	United States Customs and Border Protection Agency
CCRA	Canada Customs and Revenue Agency
CFIA	Canadian Food Inspection Agency
CI	Customs Inspector
CIC	Citizenship and Immigration Canada
CIIMS	Customs Investigations Information Management System
CIRTP	Customs Inspector Recruitment Training Program
CPO	Chief Privacy Officer
CMAA	Customs Mutual Assistance Agreement
CRA	Canada Revenue Agency
DAS	Data Acquisition System
DCS	Departure Control System
DOB	Date of Birth
DSO	Departmental Security Officer
EU	European Union
FOSS	Field Operational Support System
HQ	Headquarters
HRTI	High-Risk Traveller Identification Initiative
ICES	Integrated Customs Enforcement System
IMS	Intelligence Management System
IPIL	Integrated Primary Inspection Line (Airport)
IT	Information Technology
MLAT	Mutual Legal Assistance Treaty
MOU	Memorandum of Understanding
MRZ	Machine Readable Zone
NRAC	National Risk Assessment Centre
NTC	United States National Targeting Centre
ORS	Occurrence Reporting System
PALS	Primary Automated Lookout System (Land Border)
PIA	Privacy Impact Assessment
PAXIS	Passenger Information System
PIPEDA	Personal Information Protection and Electronic Documents Act
PTU	Passenger Targeting Unit
PURM	Privileged User Risk Management System
RIO	Regional Intelligence Officer
RIA	Regional Intelligence Analyst
SIR	Security Incident Report
TBS	Treasury Board Secretariat
TECS	United States Treasury Enforcement Communications System
TRA	Threat and Risk Assessment